JUL 14 2008

MEMORANDUM FOR DEPARTMENT OF DEFENSE EXECUTIVE AGENT FOR INFORMATION TECHNOLOGY STANDARDS
(ATTN: THE CHAIR, INFORMATION TECHNOLOGY STANDARDS COMMITTEE)

SUBJECT: Department of Defense Information Technology Standards Registry Baseline Release 08-2.0

References: (a) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004
(b) Deputy Secretary of Defense Memorandum, "DoD Executive Agent for Information Technology (IT) Standards, May 21, 2007

The DoD Information Technology (IT) Standards Registry (DISR) has been updated from Baseline Release 08-1.0 to DISR Baseline Release 08-2.0 in accordance with Reference (a). Three times a year the DISR baseline is updated to ensure the DoD capabilities for building and buying IT systems are based on a current and effective set of IT and National Security Systems (NSS) standards.

We as tri-chairs of the Information Technology Standards Oversight Panel (ISOP), acting under the authority of the DoD CIO, approve the changes to the DISR baseline listed in the attached spreadsheets as recommended by the Information Technology Standards Committee (ITSC) at their 18 June 2008 meeting. Please post the approved changes in DISR Baseline Release 08-2.0 for immediate use in DoD IT and NSS acquisitions and development systems. This Release supersedes Release 08-1.0 and contains IT and NSS standards needed to support interoperability and a net-centric operational environment.

Based on the tri-chairs' approval of DISR Baseline Release 08-2.0 and the applicable standards associated with the IPv6 Basic Standards Profile, this Profile and the document "DoD IPv6 Standard Profiles for IPv6 Capable Products – Supplemental Guidance," Version 3.0, dated 13 June 2008 are approved for distribution via the DISR.

We extend our thanks once again to the members of the ITSC and the Technical Standards Working Groups for their involvement and contributions to the DoD standards process.

BRIAN G. WILCZYNSKI	MICHAEL J. BASLA	KRISTEN J. BALDWIN
Director	Brigadier General, USAF	Acting Director
Enterprise Architecture	Vice Director, Command	Systems and Software
and Standards	and Computers Systems,	Engineering
ASD(NII)/DCIO/IMI&T	Joint Staff	ODUSD (AT&L)

Copy to: DoD CIO Executive Board
ITSC Representatives

Attachment: Changes for DISR Baseline 08-2.0

DoD IPv6 Standard Profiles For IPv6 Capable Products Version 3.0

13 June 2008

Prepared by the DISR IPv6 Standards Technical Working Group
POC: Ralph Liguori, Chair IPv6 Standards TWG
E-mail Address: ralph.liguori@disa.mil

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

Table of Contents

Executive Summary

This document provides the engineering-level definition of "Internet Protocol (IP) Version 6 (IPv6) Capable" products necessary for interoperable use throughout the U.S. Department of Defense (DoD). This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. The term "IPv6 Capable Product" as used in this document, means any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Version 1.0 of this Standard Profiles document was approved by the DoD Information Standards Oversight Panel (ISOP) in 2006 under the authority of the DoD Chief Information Officer (CIO) to "provide guidance to DoD Components and Services responsible for procuring/acquiring IPv6 Capable Global Information Grid (GIG) products" [6] as was the Version 2.0 revision in 2007 [18]. Final review and approval of this revision will be similarly documented.

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The goal of this document is to organize and summarize the requirements included by reference for the convenience of a broad spectrum of readers, including acquisition officers, testing organizations, DoD systems developers and vendors.

This document as a whole defines a set of DoD IPv6 Standard Profiles (Profiles) for IPv6 Capable Products of various classes of equipment or software, and variety of IPv6 network roles. First, Product Classes are defined that will be used in the document to group products according to their role in a network architecture. Then the Base Requirements that apply to all IPv6 Capable Product Classes are defined. Several Functional Requirements blocks are defined for specific functions performed by some products. Finally, Product Class Profiles are defined in terms of the Base Requirements and Functional Requirements.

References, a Glossary and an Appendix with a summary of the requirements in tabular form are provided at the end of the text. Appendix D provides a summary of changes with respect to the previous version of this document.

1 Introduction

The Internet Protocol (IP) is the network layer for the interconnection of packet-switched networks. The current version of IP in widespread use is IP version 4 (IPv4) first defined and deployed over 25 years ago. IP version 6 (IPv6) is a replacement for IPv4 first proposed in 1996 by publication the Internet Engineering Task Force (IETF) of Request for Comments (RFC) 2460 and a series of supporting RFCs. U.S. Department of Defense (DoD) policy mandating use of IPv6 was promulgated in “Internet Protocol Version 6 (IPv6) Interim Transition Guidance” [1] published by the DoD Chief Information Officer (CIO) John Stenbit in September 2003.

1.1 A Definition of “IPv6 Capable Product”

A Memorandum issued by the Assistant Secretary of Defense – Networks and Information Integration (ASD(NII)) entitled “Internet Protocol Version 6 (IPv6) Policy Update” [8] states that:

> “IPv6 ‘capable’ is defined as a system or product capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to IPv4. Criteria to be considered IPv6 capable are: conformant with the IPv6 standards profile contained in the DoD IT Standards Registry (DISR); maintaining interoperability in heterogeneous environments with IPv4; commitment to upgrade as the IPv6 standard evolves; and availability of contractor/vendor IPv6 technical support.”

Version 1.0 of this document was approved by the DoD Information Standards Oversight Panel (ISOP) [6] as representing the “IPv6 Profile” taking the place of the Generic IPv6 Profile in the DISR. Version 2.0 was similarly approved by the ISOP [18]. Thus, this document in its entirety provides a detailed definition of an “IPv6 Capable Product” by enumerating the requirements that must be met by a particular product for it to be considered IPv6 Capable consistent with the ASD (NII) policy update cited in the previous paragraph. While other terms such as “IPv6 Ready” or “IPv6 Compliant” have been used in other contexts, the term “IPv6 Capable Product” as it is defined in this document should be used in conjunction with a citation of this document to be clear about what is required.

The official released text of this document when approved will be posted at https://disronline.disa.mil. Access to the document on DISRonline requires a CAC card, log on, and selecting the Guidance tab. The document will also be available without access restriction at http://jitc.fhu.disa.mil/apl/.

1.2 Document Goals and Purpose

This document provides a technical and standards based definition of interoperability requirements for IPv6 Capable Products to be used in DoD networks. This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD

Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. Version 2.0 of this document was reviewed and approved by the ISOP as guidance for the acquisition of IPv6 Capable Products [18] and when approved, this version will replace Version 2.0.

RFC 4294 "IPv6 Node Requirements" published by the IETF in April 2006 has been an essential guide in the preparation of this document. The following goal statement from that RFC can also serve as the basis for the goals of this document:

> "The goal of this document (RFC 4294) is to define the common functionality required from both IPv6 hosts and routers. Many IPv6 nodes will implement optional or additional features, but this document summarizes requirements from other published Standards Track[1] documents in one place.
>
> This document tries to avoid discussion of protocol details, and references RFCs for this purpose. This document is informational in nature and does not update Standards Track RFCs.
>
> Although the document points to different specifications, it should be noted that in most cases, the granularity of requirements are smaller than a single specification, as many specifications define multiple, independent pieces, some of which may not be mandatory."

Likewise, this document does not intend to define or mandate new requirements nor to unduly restrict use of optional requirements, but to summarize the requirements for IPv6 Capable Products. To facilitate interoperability:

1. A device should not rely upon or assume the implementation of optional features in other devices for basic interoperability;

2. A device should, when feasible, implement optional features that may be useful in some deployments;

3. While a device may implement any optional features not specifically forbidden in this document, the implementation should not interfere with another device implementing required and permitted features.

For example, while Mobility is a conditional requirement, and thus optional, products that support Mobility should be interoperable with products that do not support Mobility.

[1] Standards Track is an IETF term indicating that an RFC is published with the intention that it will become an Internet Standard when mature and widely implemented. An RFC is usually published as a "Proposed Standard" and is promoted to "Draft Standards" before being considered for Internet Standard status. Further explanation of this process can be found in RFC 2026.

Typically, a feature like Mobility must be implemented in a number of cooperating nodes in the network, necessitating selection of products that do implement the option.

1.3 Target Audience

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The topic is rather technical, and requires some background understanding by the reader of the RFCs and other references cited, but the goal of this document is to organize and summarize the requirements included by reference for the convenience of the reader. The authors hope that the document is useful to several categories of users as described in the following paragraphs.

Contracts and Acquisition

Acquisition officers and others writing purchasing and contract language may use this document as a reference when they develop specific product and system requirement text. For their purposes, this document aims to adequately summarize the technical requirements such that it is sufficient (with the citation of RFCs and other specifications referenced by this document) to specify the minimal requirements for products to be IPv6 Capable. The IPv6 Capable Registry and the test reports generated during testing by the Joint Interoperability Test Command (JITC) will provide useful input to the responsible component or program acquisition effort.

Testing and Certification Organizations

DoD components will rely upon testing organizations including the Joint Interoperability Test Command (JITC) to evaluate vendor products and DoD systems as IPv6 Capable. These testing organizations may use this document as an outline and starting point for the development of detailed test plans appropriate to each product class. They will need to go beyond the summary level of this document through reference to the specifications and other technical material cited.

Developers

The engineers and managers responsible for systems development by DoD and vendor organizations may use this document as an additional check on interpretation of the specifications and other technical material cited to develop systems architectures, designs and implementations to assure that their products will be IPv6 Capable. By following the requirements documented herein, they will increase the probability that the systems they build will be interoperable with other DoD IPv6 Capable network elements and will be ready for DoD testing.

1.4 Requirement Sources

The immediate reference for requirements in this document is the Defense Information Systems Registry (DISR). The DISR is a snapshot of the state-of-practice for technical publications being tracked by DISA for inclusion in profiles for products to be acquired by DoD. These technical publications come from a number of sources, primarily external Standards Development Organizations (SDOs) and are reviewed and considered by the DoD IT Standards Committee (ITSC) and a number of DoD IT Standards Technical Working Groups (TWGs). When standards are sufficiently mature, they are added to the DISR database.

In particular, IPv6 specifications and related standards are published by the Internet Engineering Task Force (IETF) as Requests for Comments (RFCs). These documents are reviewed and analyzed by members of the IPv6 Standards TWG, and considered for mandatory or optional use in DoD systems and networks when they are stable and mature and determined to be appropriate requirements for use by DoD. Each of the RFCs cited in the DISR and in this document is included by reference in its entirety, except where this document notes exceptions or extensions. RFCs can be freely obtained through the RFC Editor by searching on the RFC number or keywords.

The DISR is updated 3 times a year after due consideration of new and replacement RFCs by the IPv6 Standards TWG. This document is coordinated with the content of the DISR database at the time of its publication, and will be updated and republished as necessary to maintain this correspondence.

In February 2007, the National Institute of Standards and Technology (NIST) released a draft for public comment entitled “A Profile for IPv6 in the U.S. Government” [9]. The NIST Profile for IPv6 was updated and circulated again in January 2008 [19]. That document is intended for U.S. Government environments exclusive of the DoD. While we have worked with the authors of that document to minimize differences between the documents, they will remain parallel efforts for the foreseeable future. Per the cited DoD policy statements [1] [2] [8] DoD acquisition of products for IPv6 deployment should follow this document and all DoD testing and certification is coordinated by the DISA Joint Interoperability Testing Command (JITC). Discussions between NIST and DoD on compatible testing programs continue; however, there are no significant differences in functional requirements as of the currently circulating drafts meaning that products approved under one program are highly likely to be interoperable with products approved under the other. There are minor differences in the effective dates of some requirements that will naturally converge over time. While there are more stringent DoD IPsec requirements (RFC 4869) that NIST deem inappropriate for civilian use, the basic IPsec RFCs define a sufficient set of compatible mandatory algorithms.

1.5 Terminology Used in This Document

The DISR database and IETF RFCs use different terminology to describe requirements. RFCs and other technical publications referenced in the DISR as standards are assigned to one of 3 statuses:

EMERGING: An EMERGING standard is a new or evolving standard that is likely to eventually become a MANDATED standard.

MANDATED: A MANDATED standard is a stable and mature standard that can be cited as a requirement in acquisition. One of the considerations for determining maturity of a standard is the existence of vendor implementations.

RETIRED: A standard that has been replaced by a newer standard or otherwise determined to be no longer appropriate for use in DoD systems is a RETIRED standard.

Additionally, RFCs or other publications can be referenced in the DISR as **INFORMATIONAL/GUIDANCE** meaning that they provide useful information that is not a standard.

IETF terminology for use in RFCs is defined in RFC 2119 including the terms MUST, SHOULD, and MAY. To provide a common lexicon, the following six terms used in this document are to be interpreted as follows:

MUST: This term indicates an imperative; the requirement is essential to IPv6 capability and interoperability. This level of requirement is indicated in the DISR by MANDATED. Synonyms used in other contexts include Threshold, SHALL or REQUIRED.

MUST NOT: This term indicates an absolute prohibition of a behavior. A synonym is SHALL NOT.

SHOULD: This term indicates a desirable or expected course of action or policy that is to be followed unless inappropriate or cost-prohibitive for a particular circumstance. This corresponds to the EMERGING[2] level in the DISR. In other contexts, the term Objective is used.

SHOULD NOT: This term is used to indicate that the particular behavior is discouraged though not prohibited. There may be valid reasons in particular circumstances when the behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing.

MAY: This term denotes the permissive or that an item is truly optional. An implementation which does not include a particular option MUST interoperate with another implementation which does include the option. In the same vein, an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (in both cases without the feature the option provides). Normally standards that a product MAY follow would be listed in the DISR as INFORMATIONAL.

SHOULD+: This term indicates a near-term goal for technology insertion that is strongly expected to be elevated to a MUST or MANDATED in the near future (see

[2] A standard that is listed in DISR as MANDATED could also be used in SHOULD, SHOULD+ and MAY clauses.

paragraph 1.5.1). SHOULD+ means a strongly recommended and expected course of action or policy that is to be followed unless inappropriate for a particular circumstance. This term is normally associated with an EMERGING specification in the DISR.

1.5.1 Effective Dates for Mandate of New and Revised RFCs

IPv6 is defined by an active and evolving set of RFCs. In addition to new emerging standards, existing standards are occasionally updated by RFCs that extend or elaborate the standards, and on occasion standards may be rendered obsolete by revised RFCs. In IETF practice, once published, an RFC is never modified; the technical material it defines can only be changed by publication of another RFC. The RFC Editor web page tracks all RFCs, and relates them to other RFCs that update or obsolete them.

The obsolescence and replacement of RFCs by new RFCs complicates a simple and clear definition of the mandatory requirements in this Standard Profiles document. There will be a period of time during which commercially available products may support either or both of the versions of the standard. In some cases the requirement is to support the *function*, preferably complying with the emerging replacement RFC but at least according to the previously published RFC. In these situations, the old and new standards will be discussed together in this document with exceptions or conditions noted, to provide clear guidance to vendors for implementation and testing.

In prior version, this specification did not provide for "in effect" dates for new or strengthened requirements, implying that they were always "effective immediately" when stated as a MUST. Recognizing realistic product cycles, the following policy is established effective with the final publication of Version 3.0:

1. An emerging requirement will typically be stated as a SHOULD+ when it is first cited in a revision of this specification, indicating that it is likely to be strengthened to a MUST in the next revision nominally 12 months later; in exceptional circumstances the first citation of a requirement may be a MUST;

2. A "grace" period of 12-24 months will be allowed between the statement of a new or strengthened MUST requirement in a revision of this specification and enforcement of the mandate;

    a. Nominally, a replacement RFC will have an effective date 12 months following its first citation as a MUST; In some cases, the *function* specified in a set of revised and obsolete RFCs MUST be supported, preferably according to the revised RFC, but minimally at the prior RFC;

    b. Nominally, a new functional requirement will have an effective date 24 months following the first citation as a MUST; this recognizes the more significant development effort for a new feature rather than an update based on a revised specification for an existing capability;

3. Exceptions for specific requirements will be noted in the text, where a longer or shorter allowance is appropriate; in all cases, the Effective Date column in the Appendix C Requirements Summary will provide an unambiguous indication of the effective date;

4. Requests for dispensations beyond the stated policy will be evaluated on a case-by-case basis by DISA Standards Engineering and JITC. The ultimate authority for waiver of any requirement for IPv6 Capable products will be defined by the component making the purchase and deployment decision.

The Requirements Summary Table in Appendix C includes a column to indicate the effective date for each requirement in the text.

1.5.2 Distinction Between Capability and Deployment

Throughout this document the terms “support” and “implement” as well as other forms of the words such as “supported”, “implementation”, etc. are used to indicate that a requirement or function is available in a product. In other words, the compliant product is capable of providing the function. For example, if a product class MUST support MLDv2 as defined in RFC 3810, a compliant product of that class meets the requirements in that RFC to provide MLDv2 function. This does not imply that the available function will be actively used. The terms “deployment” and “use” as well as other forms of those words indicate active operation of an available capability or function.

1.5.3 Conditional Requirements

Note also that some requirements clauses or paragraphs of this specification may be applied conditionally. The language in these instances is intended to be self-explanatory, and stated as simply as possible to capture the technical nuances, for example as used in Section 3.1.1:

> “An IPv6 Capable Host/Workstation…Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node.”

This should be read to mean that the requirement to support the sections of the RFCs for MIPv6 Mobile Node functionality would not be mandatory for all IPv6 Capable Host/Workstation Products, but is mandatory for products that are intended to operate as a Mobile Node in a MIPv6 deployment. Submission and test results for a product will note whether or not the product includes any of the conditional requirements. For example, “Product X meets the requirements for an IPv6 Capable Host/Workstation with Mobility” indicates that Product X complies with all the basic requirements for Host/Workstation and also meets the requirements for a MIPv6 Capable mobile node. On the other hand “Product Y meets the requirements for an IPv6 Capable Network Appliance” indicates that Product Y only meets the basic requirements for a Network Appliance.

1.6 IPv6 Capable Product Classes

Before examining detailed requirements it would be useful to frame the discussion by defining the classes of IPv6 Capable Products. The terminology used in the IPv6 base specification [RFC 2460] only defined two very general classes of nodes. Describing the requirements for a specific IPv6 Capable product using those broad classes would require complex exceptions and explanations to distinguish among different products. This Standard Profiles document groups IPv6 Capable Products into a small number of Product Classes convenient for defining common requirements. IPv6 Capable Products are classified according to their architectural and functional role in an IPv6 network**:**

- **End Node:** A node processing IPv6 packets addressed to the node itself or originating IPv6 packets with a source address of the node itself.
    - **Host/Workstation:** a personal computer (PC) or other end-user computer or workstation running a general purpose Operating System (OS) such as UNIX®[3], Linux®[4],Windows®[5], or a proprietary operating system that is capable of supporting multiple applications. A Host/Workstation typically has a single user, with a local (console) login, and is generally managed by the end-user (or the end-user organization support team, rather than the Internet Service Provider (ISP) or other third party).

      Note that a Host/Workstation can be viewed as a hardware platform combined with its OS; however, the implementation of the IPv6 Capability in one embodiment is that the operating system (OS) implements IPv6 and it is independent of the hardware platform. In fact the particular hardware platform running the OS is usually irrelevant; for example, Microsoft Windows Vista running on any PC has the same IPv6 capabilities. The PC running Windows Vista in this case, whether HP, Dell or custom-built has no IPv6 capability of its own independent of the OS. The implementation of the IPv6 Capability in a second embodiment consists of the OS that works with a hardware implementation of the IP stack (usually a network interface card). Thus an OS and a network interface card with an IPv6 hardware implementation may entirely implement IPv6 capability and thus run on any particular hardware platform. Overall, this note may apply to products in any of the Product Classes.

[3] *UNIX® is a registered trademark of The Open Group*

[4] *Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.*

[5] *Windows® is a registered trademark of Microsoft Corporation in the United States and other countries.*

  - **Network Appliance or Simple Server**[6]**:** Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A **Network Appliance** is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface. A **Simple Server** supports a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)[7] servers, a "web camera" appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests. A device with a trivial or no role at the IP layer, for example a modem or layer 2 switch, may have a user or management interface with an IPv6 address. These devices should also be evaluated as a Network Appliance/Simple Server.

  - **Advanced Server:** End Nodes with one or more server-side applications (for example Dynamic Host Configuration Protocol (DHCPv6), Domain Name Server (DNS), Network Time Protocol (NTP), E-mail, File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), web server, storage server or database) to support clients in the network. Servers are usually managed by network administrators or operated by a third party such as an ISP or other vendor. An **Advanced Server** typically runs a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operating system and is capable of serving any number of applications to many concurrent clients.

- **Intermediate Node:** A node that forwards IPv6 packets not explicitly addressed to the node itself.[8]

  - **Router:** An Intermediate Node that forwards packets based on paths discovered using routing protocols. A router typically has a small number of ports to interconnect several networks, in particular to connect a Local Area Network (LAN) to a Wide Area Network (WAN). A Router implements complex control plane functions, including routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol

[6] The distinction between Simple Server and Network Appliance results in no real difference in requirements or testing. Simple Server product class could be eliminated completely, but is retained for consistency with previous revisions and test results.

[7] See RFC 3261 Session Initiation Protocol for more information on SIP

[8] Please note that an Intermediate Node may also act as an End Node for Network Management and other protocols, and must conform to Simple Server functionality for IPv6 packets addressed to an IPv6 address of the node itself.

(BGP) which are typically implemented in software run on a general purpose CPU.

- **Layer-3 Switch:** An Intermediate Node that forwards IPv6 packets at switching speeds usually through the use of special purpose dedicated hardware. A Layer-3 Switch typically has a higher port density than a Router and is intended to interconnect end-nodes in a LAN environment. A Layer-3 Switch may have some limited layer-3 control plane (management or routing) functions but is primarily a data plane device. A Layer 2 switch is transparent at the IP layer, and as such plays no active role as an IPv6 Capable product. However, the device may be managed over an IPv6 interface and should be evaluated as a Simple Server.

- **Information Assurance Device:** An Intermediate Node that performs a security function as its primary purpose by filtering or encrypting network traffic, and which may block traffic when security policy dictates. For example a Firewall, Intrusion Detection System, Authentication Server, Security Gateway, High Assurance IP Encryptor (HAIPE) or Virtual Private Network (VPN) is Information Assurance Devices. A Router or Layer 3 (L3) Switch may incorporate an IA function in addition to its primary role, but is not an IA Device but rather an "IA Enabled" product. .

- **IPv6 Capable Software:** a product that implements functions available via an IPv6 interface to end-users, network nodes or other software, when installed on an appropriate hardware platform. Section 4 of this document introduces some concepts for the evaluation of pure software IPv6 Capable products (operating systems or applications) but a full definition of IPv6 Capable Software Product Classes is deferred to a future revision of this document.

Some of the terms used in this document for defining Product Classes have been used with different definitions in the networking industry, but throughout this document and in references to this document, the terms are intended to be used as defined above. In particular the term Network Appliance has been used for a variety of End Node and Intermediate Node products, and is the name of a storage solutions company.

We have attempted to make the distinctions between Product Classes as objective as possible, but some of the differences are subject to interpretation, in particular the classification of a Server product as "Simple" or "Advanced". It is essential that a vendor come to agreement with the testing organization (JITC for example) on proper classification of their product before testing. The testing organization and the Chairman of the DISR IPv6 Standards TWG can be of assistance in classifying products that don't obviously fit one of the Product Classes. Many products include other interfaces in addition to the IPv6 interface, such as a Voice-over-IP (VOIP) device or Circuit-to-Packet (CTP) device. Such a device can be evaluated as a "black box" from its IPv6 interface, without regard to other internal or external non-IPv6 interfaces.

The following table summarizes the Product Class definitions and characteristics to help with the classification of specific products. For example, if the product is an End Node, managed by the End-User organization, accessed by a single user through a local interface rather than remotely via a Web interface, it is best identified as a Host/Workstation.

	Host/ Workstation	Network Appliance	Advanced Server	Simple Server	Router	Layer 3 Switch	Information Assurance Device
End Node	Yes	Yes	Yes	Yes	Optional	Optional	Optional
Intermediate Node	No	No	No	No	Yes	Yes	Yes
End-User Managed	Yes	Yes	No	No	No	No	No
Web Access	No	Optional	Optional	Optional	Optional	Optional	Optional
Local login or console	Y	Optional	Optional	Optional	Optional	Optional	Optional
Loadable or Embedded	Loadable[9]	Embedded	Optional	Embedded	Optional	Optional	Optional
Number of Applications	Many	Few	1 to Many	Few	unspecified		
Number of Users	1	1 to F	Many	Few			
Network Interconnection	Not applicable				Yes	No	Not Applicable
Port Density					Low	High	
Complex Control Plane					Yes	No	
IA Function					Optional	Optional	Yes

Table 1-1: Product Class Summary

[9] A Host/Workstation is typically "loadable" although in practice, some systems may be preloaded by an administrator with the end user restricted from loading additional software.

2 IPv6 Capable Product Requirements

This section identifies the specifications that will be used to define the requirements for the Product Classes outlined above. These specifications are organized into several functional categories. First, the Base Requirements are defined, comprising the standards that will (with minor exceptions) apply equally to all Product Classes. Then, a set of Functional Requirements categories are defined, which will be used as "building blocks" to construct the detailed Product Class Profiles in Section 3.

Specific requirements in the RFCs cited in the Base or Functional Requirements may in some cases apply in the same manner to IPv6 End Nodes and IPv6 Intermediate Nodes or may apply differently to each class; the language in this document is intended to make these distinctions clear. The reader may read the cited RFCs for a more detailed understanding of the specific requirements. Extensions, restrictions and exceptions with respect to the Product Classes defined in this document can be found in Section 3.

While this document is intended to cover the preponderance of products to be used in DoD networks and applications, the authors recognize that programs may have circumstances that justify the extension, modification or exception to requirements in this document by means of program-specific documentation. For example, the Real-Time Services (RTS) program defines some unique appliances and products for use in the Defense Switched Network (DSN) and the Defense Red Switch Network (DRSN). RTS/DSN/DRSN components such as the Local Session Controller (LSC), IP Enabled End Office (EO) and Edge Boundary Controller (EBC) will be IPv6 capable as specified in this document with exceptions and design/implementation guidelines noted in latest version of the DoD Unified Capabilities Requirements (UCR) document.

2.1 Base Requirements

These Base Requirements are the core of interoperability requirements for IPv6 Nodes.

- All IPv6 Nodes MUST conform to RFC 2460, Internet Protocol v6 (IPv6) Specification, as updated by RFC 5095 – Deprecation of Type 0 Routing Headers in IPv6; this is the fundamental definition of IPv6.
- All IPv6 Nodes MUST implement RFC 4443, Internet Control Message Protocol (ICMPv6).
- All IPv6 Nodes MUST implement RFC 4861 – superseding RFC 2461, Neighbor Discovery (ND) for IPv6, as appropriate to their role as an IPv6 End Node or IPv6 Intermediate Node. Informational RFC 4943 provides additional background on implementation of ND. Also note that ND implies that nodes MUST support Multicast Listener Discovery (see below).
- All IPv6 Nodes MUST operate with the default minimum Path MTU (PMTU) size of 1280 octets as defined in RFC 2460. All IPv6 Nodes SHOULD support a minimum PMTU of 1500 to allow for encapsulation. All IPv6 Nodes except Network Appliance/Simple Server MUST implement RFC 1981, Path MTU Discovery for IPv6.

- All IPv6 Nodes MUST provide manual or static configuration of its IPv6 interface address(es).
- An IPv6 Node which supports an autonomous method for discovering its own unique IPv6 interface addresses (see section 2.9) MUST have the means to disable the autonomous method to force manual or static configuration of addresses, e.g. the user can disable the "Creation of Global and Site-Local Addresses" as described in Section 5.5 of RFC 4862 (replaces RFC 2462 as of Version 3.0 of this document) on an IPv6 Node that supports Stateless Address Autoconfiguration (SLAAC).
- While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes MUST support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862; DAD MUST NOT be disabled.
- All IPv6 Nodes MUST support the IPv6 Addressing Architecture as defined in:
  - RFC 4291, IPv6 Addressing Architecture[10]
  - RFC 4007, Scoped Address Architecture (All IPv6 addressing plans MUST use this standard definition for scoped addressing architectures; however, support for zone indexes is optional)
  - Additional guidance may be found in RFC 5156 – Special Use IPv6 Addresses which documents addresses with special purposes in various protocols, including some that should not appear on the public Internet
- An IPv6 Node MAY support RFC 4193, Unique Local IPv6 Unicast Addresses (ULA), which replaces the site-local address with a new type of address that is private to an organization, yet unique across all of the sites[11] of the organization. Nodes are not required to support ULA at this time.
- All IPv6 Nodes MUST implement Multicast Listener Discovery (MLD)
  - Neighbor Discovery (ND) is a core feature of IPv6, analogous to ARP in IPv4, and is therefore a fundamental requirement for IPv4 parity. ND uses link-layer Multicast for some of its services; therefore ALL IPv6 Capable products will be using Multicast. In addition, switches may include the "MLD Snooping" feature that will block multicast addresses that are not registered with MLD. This means that products lacking MLD support cannot guarantee that ND will work in all deployments.
  - At a minimum all nodes MUST follow RFC 2710, Multicast Listener Discovery for IPv6 and SHOULD+ support the extended MLDv2 as in RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6.
  - All IPv6 Nodes SHOULD+ follow the source address selection rules in RFC 3590 – Source Address Selection for the Multicast Listener when MLD is used, per RFC 4294 section 4.6.

[10] Also see the current Internet-Draft http://tools.ietf.org/html/draft-ietf-v6ops-addcon-07 and the DoD Addressing Plan [14]

[11] RFC 3879 "Deprecating Site Local Addresses"

2.1.1 Connection Technologies

All IPv6 Nodes conditionally MUST support a connection technology (link layer) that can carry IPv6 packets, consistent with its intended deployment. When using a connection technology with a published "IPv6 over" standard, the device MUST follow the corresponding standard for interoperability across that connection technology. Most IPv6 Capable products will implement one or more of the following standards:

- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;
- RFC 2492, IPv6 over ATM Networks;
- RFC 5072 (replaces RFC 2472), IP Version 6 over PPP;
- RFC 3572, IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH).
- RFC 2467, Transmission of IPv6 Packets over FDDI Networks;
- RFC 2491, IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks;
- RFC 2497, Transmission of IPv6 Packets over ARCnet Networks;
- RFC 2590, Transmission of IPv6 Packets over Frame Relay Networks Specification;
- RFC 3146, Transmission of IPv6 over IEEE 1394 Networks;
- RFC 4338, Transmission of IPv6, IPv4 and Address Resolution Protocol (ARP) Packets over Fibre Channel;
- RFC 4944, Transmission of IPv6 Packets Over IEEE 802.15.4 Networks (Low Power Networks)

2.2 IP Layer Security (IPsec) Functional Requirements

Security is a complex topic and the role of IP Layer Security (IPsec) within the overall DoD approach to security is still evolving. The DoD transition to IPv6 requires IPsec as part of the toolkit to build secure networks, but this does not preclude the use of other security methods. Secure Socket Layer (SSL), HTTP over SSL (HTTPS), Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) will continue to be appropriate for some deployments.

There are several dimensions to the treatment of IPsec in this set of profiles:

1. For IPsec to be useful as a security tool it must be generally available and devices in the network cannot interfere with its use[12]; IPsec has long been considered a core part of IPv6 Capable products as recognized in RFC 4294 – IPv6 Node Requirements;

2. A node's responsibilities with respect to IPsec must be considered in the architectural context; a Router or Switch does not perform IPsec as part of normal traffic forwarding; however, it may implement IPsec when it is acting as

[12] A firewall or other IA Device might be configured to block IPsec but would not inherently "interfere" with the deployment of IPsec otherwise.

an End Node in some deployments for network management and in routing protocols; if an Intermediate Node integrates IPsec capability to protect traffic it forwards, that Node becomes a special-purpose IA Enabled device functioning as a Security Gateway; alternatively, this function might be provided by an outboard cryptographic device;

3. Products are required to support IPsec so that it is available for use; however, this document does not require its activation or use; activation of IPsec or waiver of IPsec requirements is a deployment decision; effective use of IPsec in a particular deployment may also be dependent on integration with other elements, including IPsec-aware applications;

4. NSA opinion that any device implementing encryption with IPsec is an Information Assurance (IA) device subject to Federal Information Processing Standards (FIPS) and National Information Assurance Partnership (NIAP) certification may be an impediment to wide vendor support but this is beyond the scope of this document. NIST publication [6] on this subject implies that a vendor may rely on previously approved and available cryptographic modules (hardware or software) integrated with their product to avoid certification of their product set as a new IA Device.

After due consideration of the above points, the IPv6 Standards TWG consensus was to maintain the strong requirement for IPsec at the current published standards as was stated in Version 1.0 and reiterated in Version 2.0. The intention is to prevent the proliferation of IPsec deficient products that may interfere with DoD ability to fully utilize IPsec. The Product Class Profiles in Section 3 identify which Product Classes MUST be IPsec Capable; however, all IPv6 Capable products SHOULD+ be IPsec Capable. IPsec Capable requirements are:

1. IPsec Capable products MUST support the current RFC 4301 Architecture as defined in Section 2.2.1.

2. IPsec Capable products MUST support Manual Keying and MUST support Internet Key Exchange Version 2 (IKEv2), as defined in Section 2.2.2.

3. IPsec Capable products SHOULD support RFC 3971, Secure Neighbor Discovery (SEND) and RFC 3972 Cryptographically Generated Addresses (CGAs)[13].

4. Conditionally, where security requirements prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPsec Capable

[13] There are some intellectual property rights concerns with CGA and use of CGA in SEND; although the rights are offered on a "Royalty-Free, Reasonable and Non-Discriminatory License to All Implementers", the fact that a license is required may hinder adoption by some vendors.

products MUST support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Auto configuration in IPv6.

Further guidance for network security can be found in RFC 4942 – IPv6 Transition/Co-existence Security Considerations and RFC 5157 – IPv6 Implications for Network Scanning. Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection.

A waiver process outside the scope of this document may be available (as determined by DoD component) to allow use of a product that does not at this time support the IPsec requirements as defined in this document for its Product Class Profile. However, we recognize that implementation of IPsec Version 3 and IKEv2 is not prevalent at this time. Products that do not meet these standards MUST at least meet the fallback requirements defined in paragraph 2.2.3.

2.2.1 RFC 4301 Architecture

A set of RFCs defining the Security Architecture for IP and supporting protocols was published in November 1998, and became the de facto standard for security in IPv6 products (RFC 2401 et al, referred to as IPsec Version 2 or the RFC 2401 Architecture). This set of standards was rendered obsolete (for the most part) by a set of revised standards in December 2005 (RFC 4301 et al, referred to as IPsec Version 3 the RFC 4301 Architecture).

All IPv6 Nodes implementing IPsec RFC 4301 Architecture MUST support the Security Architecture for the Internet Protocol as defined in RFC 4301 and as well:

- MUST support the Encapsulating Security Payload (ESP) defined in RFC 4303;
- SHOULD support RFC 4302, IP Authentication Header (AH);
- MUST implement ESP and AH cryptography as defined in RFC 4835 (replaces RFC 4305), Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).

IPv6 Nodes MUST support suites of cryptographic algorithms for IPsec and IKE including:

- Suite VPN-B in RFC 4308 – Cryptographic Suites for IPsec;

- Suite-B-GCM-128 (for encryption plus authentication) in RFC 4869 – Suite B Cryptographic Suites for IPsec

- Suite-B-GMAC-128 (for authentication only) in RFC 4869 – Suite B Cryptographic Suites for IPsec.

Conformance with these cryptographic suites will ensure that all IPsec implementations for DoD approved products support an interoperable set of options. These RFCs do not introduce new algorithms, but detail a subset of other referenced RFCs. RFC 4869

MUST be used as guidance in the interpretation of the RFCs that it references. Nodes MAY support additional cryptographic suites and options where appropriate to the deployment and application but MUST NOT depend on other nodes support. Additional guidance can be found in RFC 4308 and NSA publications on Suite B including the Fact Sheet available at http://www.nsa.gov/ia/industry/crypto_suite_b.cfm.

IPv6 Nodes in deployments requiring strong Advanced Encryption Standard (AES) security across wireless links SHOULD support AES Counter with Cipher-block Chaining Message Authentication Code (CCM) Mode as specified in IEEE 802.11-2007 amendment 802.11i wireless security standard. [16] [17]

The requirement for RFC 4301 Architecture for IPsec is effective with publication of Version 3.0, which is 24 months from specification of MUST for this requirement in Version 1.0 of this document. It is strongly recommended that all products meet this requirement before submission for IPv6 Capable testing. While a product may be on the IPv6 Capable Registry with an exception, DoD components may have specific deployment requirements that prevent them from buying products that do not meet the IPsec requirements.

2.2.2 IKE Version 2 Support

In conjunction with the IPsec Architecture, some method for key management is required. All IPv6 Nodes implementing IPsec need to be interoperable with Product Classes that only support Manual Keying (especially Network Appliances and Simple Servers). Therefore all IPv6 Nodes MUST support Manual Keying for IPsec.

Internet Key Exchange (IKE) was defined in RFC 2409 but has been rendered obsolete by IKE Version 2 (IKEv2). IKEv2 is simpler to deploy, has clearer documentation, is more efficient, has fewer options and fixes some of the shortcomings in IKEv1. IKEv2 is integral to the RFC 4301 Architecture and some of its advanced features depend on IKEv2 and are not available with the original IKE.

IKE Version 2 (IKEv2) is defined in the following referenced RFCs. An IPv6 Node implementing IKEv2 MUST support:

- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

In addition, RFC 4718 provides guidance and clarification for IKEv2 implementations.

IKEv2 by design is not interoperable with IKEv1 implementations. Products implementing IKEv2 MAY implement an operational fall-back to IKEv1 to provide interoperability.

The requirement for IKEv2 has an effective date of July 2010, which is 24 months from the publication of Version 3.0 of this document, reiterating the MUST first stated in Version 2.0. This specification delays the effective date for IKEv2 based on the current lack of support in commercial products and vendor feedback. It is still strongly recommended that all products meet this requirement before submission for IPv6 Capable testing, and if not the vendor Letter of Conformance (LoC) SHOULD include a statement of future support. While a product may be on the IPv6 Capable Registry with an exception, DoD components may have specific deployment requirements that prevent them from buying products that do not meet the IKEv2 requirements.

2.2.3 IPsec and IKE Fall-back Requirements

A product in a product class that MUST support IPsec which does not implement IKEv2 may be approved with an exception, but in such a case the product MUST at least support the legacy automatic Internet Key Exchange (IKE) original version by supporting the following RFCs

- RFC 2407, The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408, Internet Security Association and Key Management Protocol
- RFC 2409, The Internet Key Exchange (IKE)
- RFC 4109, Algorithms for Internet Key Exchange Version 1 (IKEv1)
- SHOULD support RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).

A product in a product class that MUST support IPsec RFC 4301 architecture may be approved with an exception, but in such a case the product must support the following fallback requirements for RFC 2401 architecture:

- All nodes MUST support the Security Architecture for the Internet Protocol as defined in RFC 2401
- All nodes MUST support the IPsec Encapsulating Security Payload (ESP) as defined in RFC 2406
- All nodes MUST support the IPsec Authentication Header (AH) as defined in RFC 2402,

Although this version of IPsec is RETIRED, this definition is included to help evaluate legacy products that will not meet the 4301ARCH.

2.3 Transition Mechanism (TM) Functional Requirements

The long-established strategy for IPv6 transition depends on achievement of “IPv6-dominance” before the exhaustion of IPv4 address space. In an IPv6-dominant network the preponderance of end-nodes would be IPv6 Capable, all routers would be Dual Stack, and the majority of traffic would be IPv6. IPv6 Capable end-nodes would be

Dual Stack to support communication with the residual IPv4 legacy nodes. Unfortunately, the day of reckoning (shortage or exhaustion of IPv4 address space) will arrive before the achievement of IPv6-dominance. The provision of significant routable IPv4 address space to support large numbers of Dual Stack end-nodes is difficult already, and will become impossible as registries restrict allocation and eventually run out. Dual Stack will not be feasible for some network operators (e.g. broadband access networks that would require a large pool of IPv4 addresses for new Dual Stack subscribers) and significant new effort is in progress in the IETF IPv6 Operations (v6ops) working group to define viable alternatives to transition that will not require IPv4 address space. While such developments will be of interest to DoD, the exhaustion of IPv4 address space will not significantly impede the deployment of Dual Stack hosts within DoD networks due to the large pool of IPv4 addresses already allocated.

Recognizing that IPv6 Nodes will coexist with legacy IPv4-only Nodes for some time, Transition Mechanisms (TMs) will be needed to support interoperability. There is some disagreement on the proper terminology to use but the term “transition” in the context of this document refers to the co-existence of IPv4 and IPv6 nodes in an operational network regardless of the time span. The editors are continuing to use the terms Transition and Transition Mechanism for consistency with previous versions and with other policy statements [8].

Like IPsec, TM requirements are dependent on application, deployment and architectural factors. Deployment of IPv6 must accommodate the IPv4 base, as there will be no capability for IPv4 networks or nodes to interoperate with IPv6. It is difficult to define transition requirements for a particular product – the network architecture must support the long-term interoperability of IPv6-only end-nodes with IPv4-only peers, and among the residual IPv4 networks and nodes. All new nodes being acquired for connection to the DoD Global Information Grid (GIG) must support certain transition mechanisms as described in this section, and may support others.

These mechanisms include dual stack operation, configured and automatic tunneling and translation. RFC 4213, Transition Mechanisms for IPv6 Hosts and Routers, describes several general transition strategies. Each has strengths and weaknesses and would be appropriate to particular architectural situations. To provide maximum interoperability between IPv6 Capable Nodes/Networks and IPv4 nodes/networks the following principles apply:

The core network (Routers, Switches, Information Assurance Devices and any other intermediate nodes) MUST permit transit of both IPv6 and IPv4 packets. This condition can be met through Dual Stack operation across the network (dual protocol routing) OR tunneling at the edge Router.

All IPv6 nodes SHOULD support Dual Stack to ensure interoperation with the IPv4 base at all phases of the transition. Conditionally, IF an IPv6 End Node is required to interoperate with an IPv4-Only End Node, it MUST accept and transmit IPv4 packets. This condition can be met with Dual Stack operation on the platform and dual stack support in the Application or via translation. The translation method can be internal to the platform (bump-in-the-stack), or provided in an external translation device. While Dual Stack in all nodes (including Dual Stack aware applications) is a preferred solution, some products (Network Appliance or Simple Server) may be IPv6-Only, and for some time IPv4-Only legacy devices will remain.

Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) is no longer supported in the IETF community and has been rendered *Historic* by the publication of RFC 4966 primarily for security concerns*.* NAT-PT as defined in RFC 2766 SHOULD NOT be used in operational DoD networks.[14] Mechanisms based on similar designs are being discussed within IETF and it appears that one or more of the proposals may progress to standards track; however, any solution would have to mitigate the security risks inherent to NAT-PT.

Security is a particular concern in transition mechanisms. RFC 4942 – IPv6 Transition/Coexistence Security Consideration should be consulted for guidance on the use of transition mechanisms. The use of “IPv4 Mapped” addresses “on-the-wire” is discouraged due to security risks raised by inherent ambiguities[15]. The Teredo method [RFC 4380] which allows IPv6 traffic to punch through simple Network Address Translators (NATs) raises a number of security issues that have been documented [11]. Therefore the use of IPv4 firewalls and Local Network Protection for IPv6 (RFC 4864) is strongly recommended in DoD networks. Teredo may be prohibited in some DoD networks [12].

Use of IPv4 components or a translation solution internal to a product is irrelevant to the IPv6 Capable determination. For example, a translation box that adapts an IPv4-Only legacy device by translation should be evaluated as an IPv6 Host/Workstation, Network Appliance or Server depending on its network deployment. Similarly, a complex product composed of several components may have an internal IPv4 network to connect those components, which is not visible if the “system under test” is considered to be the total complex. Only the externally visible IPv6 interface behavior is relevant to the determination of IPv6 Capability; the internal IPv4 interfaces and the IPv4 legacy devices will not be evaluated, analogous to the internal functions (bus, memory, etc.) of any device or set of devices being evaluated as a unit under test for IPv6 Capability.

Systems MAY use other approaches to transition defined in RFCs or Internet-Drafts, as long as they do not conflict or interfere with other requirements for IPv6 Capable Nodes. RFC 4852 – IPv6 Enterprise Network Analysis provides analysis of managed network scenarios that are relevant to DoD network transition. Conditionally, where IPv6-in-IPv4

[14] While there are security considerations, there are limited situations where NAT-PT could be used securely, and there were comments at IETF from some who intend to use it in their networks. This specification does not absolutely forbid NAT-PT, but any use requires a thorough understanding of the security concerns

[15] See http://tools.ietf.org/html/draft-itojun-v6ops-v4mapped-harmful-02 an expired but widely cited Internet Draft

tunneling from a Dual Stack host is needed RFC 3053, IPv6 Tunnel Broker MUST be followed. Dual Stack Routers may use automatic tunneling per RFC 4852. All Routers and L3 Switches serving as Provider Edge Router SHOULD support IPv6 over MPLS following RFC 4798, Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers.

Additional mechanisms built on top of these existing mechanisms MAY be supported. An example of this is turning a communications gateway server, such as an e-mail server, into a Dual Stacked Application-Level Gateway (ALG) that can intermediate between IPv4-only mail clients and IPv6-only mail clients.

2.4 Quality of Service (QoS) Functional Requirements

As IPv6 Quality of Services (QoS) extensions and usage guidance matures, this profile will be expanded. The following are current IPv6 protocols related to QoS signaling:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
    - Routers MUST process Differentiated Service (DiffServ) headers and offer differentiation of traffic service classes
- RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP
    - Routers SHOULD process the ECN field in the IP header
- Routers to be deployed in an Integrated Services (IntServe) architecture SHOULD+ support RSVP based QoS as defined in the following RFCs:
    - RFC 2205, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification
    - RFC 2207, RSVP Extensions for IPSEC Data Flows
    - RFC 2210, The Use of RSVP with IETF Integrated Services
    - RFC 2750, RSVP Extensions for Policy Control
- Optionally, Routers may also support RFC 3175, Aggregation of RSVP for IPv4 and IPv6 Reservations
- The following RFCs MAY be supported in some deployments:
    - RFC 3181, Signaled Preemption Priority Policy Object
    - RFC 2961, RSVP Refresh Overhead Reduction Extension
    - RFC 4495, A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow
    - RFC 2998, A Framework for Integrated Services Operation over DiffServ Networks
    - RFC 2996, Format of the RSVP DCLASS Object
    - RFC 2746, RSVP Operation Over IP Tunnels
    - RFC 3182, Identity Representation for RSVP
    - RFC 2872, Application and Sub Application Identity Policy Element for Use with RSVP
    - RFC 2747, RSVP Cryptographic Authentication

2.5 Mobility (MOB) Functional Requirements

Mobile IPv6 (MIPv6) and NEtwork MObility (NEMO) are emerging IPv6-based network mobility services that SHOULD be implemented on new IPv6 systems. Application and deployment conditions will dictate whether these optional features are required for particular configurations, so these requirements are conditional: if a capability is included, the product MUST implement it as defined in the RFCs cited for that capability. MIPv6 is defined in RFC 3775, Mobility Support in IPv6 and security for MIPv6 is defined in RFC 3776, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents as updated by RFC 4877, Mobile IPv6 Operations With IKEv2 and the Revised IPsec Architecture. NEMO is defined in RFC 3963, Network Mobility (NEMO) Basic Support Protocol.

RFC 4877 recently extended the previous definition of MIPv6 security, RFC 3776. RFC 3776 specified IKEv1 for MIPv6 security while RFC 4877 provides compatibility with the RFC 4301 IPsec architecture by specifying the use of IKEv2 with MIPv6. While the requirement on RFC 4877 is new in Version 3.0 of this specification, with an effective date 24 months following publication, we recommend that MIPv6 Capable Nodes and Home Agent Routers support IKEv2 for MIPv6 security as soon as practical.

2.5.1 MIPv6 Capable Node

An End Node which can operate as a Mobile IPv6 node is “MIPv6 Capable”. If a product will be deployed as a MIPv6 Capable Node it MUST support the Mobile Node requirements in RFC 3775, MUST support RFC 3776 and MUST support RFC 4877. A MIPv6 Capable Node SHOULD+ support RFC 4282, The Network Access Identifier and SHOULD+ support RFC 4283, Mobile Node Identifier Option for MIPv6.

2.5.2 Home Agent Router

The MIPv6 architecture defines a “Home Agent” as a Router on the Mobile Node home network which coordinates the rerouting of packets addressed to the Mobile Node. A Router that will be deployed as a Home Agent MUST support the Home Agent requirements in RFC 3775, MUST support RFC 3776, MUST support RFC 4877 and SHOULD+ implement RFC 4282 and RFC 4283.

2.5.3 NEMO Capable Router

Network Mobility (NEMO) extends Mobile Node capability to an entire sub-network. A Router which meets the requirements for Network Mobility is a “NEMO Capable Router.” A NEMO Capable Router MUST implement RFC 3963.

2.5.4 Route Optimization

Any IPv6 Capable Nodes can interoperate with a MIPv6 Mobile Node as a Correspondent Node as stated in Section 8.1 of RFC 3775 (no additional functionality is required). MIPv6 includes a feature called “Route Optimization” which increases the efficiency of packet routing between a Mobile Node and Correspondent Node. An IPv6 Capable Node to be deployed where MIPv6 is prevalent SHOULD support Route Optimization as defined in RFC 3775.

2.6 Bandwidth Limited Networks Functional Requirements

IPv6 support for RF wireless systems and other bandwidth limited deployments will benefit from optimizations including header compression. The requirements in this section are conditional; where header compression is needed, the listed RFCs MUST be followed. Please note that header compression by its nature may not be compatible with IPsec in some configurations.

2.6.1 Robust Header Compression (RoHC)

Robust Header Compression (RoHC) is designed to provide a significant improvement in transmission efficiency for bandwidth limited networks. It will likely be used in cellular networks (2.5G and 3G) and other wireless links. It is an emerging technology, and currently optional. Where it is used the following RFCs are relevant:

- RFC 3095, RObust Header Compression (ROHC) – Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.
- RFC 4815, Corrections and Clarifications to RFC 3095.
- RFC 4995, RoHC Framework – this RFC is an unmodified extract of the framework definition from RFC 3095.
- RFC 4996, RoHC: A profile for TCP/IP – this RFC provides a specific profile for compression of TCP/IP headers based on the framework defined in RFC 4995.
- For compression over various PPP and low-speed links – RFC 3241, RObust Header Compression (ROHC) over PPP.
- RFC 3843, RObust Header Compression (ROHC): A Compression Profile for IP– Additional guidance for extending RFC 3095 for any arbitrary IP header chain. Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.
- RFC 4362, RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP - Additional guidance for optimizing RFC 3095 for various link-layers. Supports reliable IP header compression over wireless links.

2.6.2 IP Header Compression

IP Header Compression is an earlier alternative to RoHC. IP Header Compression is optional, where used the following RFCs are relevant.

- RFC 2507, IP Header Compression, February 1999 (For low-speed wired links requiring compression)
- RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links (For low-speed serial links requiring compression)
  RFC 3173, IP Payload Compression

2.7 Network Management (NM) Functional Requirements

While the requirements for Network Management are still evolving, SNMP Version 3 (SNMPv3) as defined in Standard 62/RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks is the preferred method of remote management, although alternative management tools are also permitted. Conditionally, IF IPv6 Compatible Nodes are managed via SNMP the management MUST support SNMPv3 as defined in IETF Standard 62:

- RFC 3411, An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)
- RFC 3412, Message Processing and Dispatching for the SNMP
- RFC 3413, SNMP Applications

SNMP implementation is built around a Management Information Base (MIB) defined by several general MIB and protocol RFCs as well as MIB RFCs specific to a node type or specific features. Conditionally, IF IPv6 Compatible Nodes are managed via SNMP implementations MUST support the following general MIB specifications:

- RFC 3595, Textual Conventions for IPv6 Flow Label
- RFC 4022, Management Information Base for the Transmission Control Protocol
- RFC 4113, Management Information Base for the User Datagram Protocol

Other MIBs that MAY be appropriate to specific products or features include:

- RFC 4087, IP Tunnel MIB
- RFC 4293, Management Information Base (MIB) for IP, obsoletes RFC 2465 and 2466 and MUST be supported to provide SNMPv3 management of IPv6 features; these two RFCs have been combined with IPv4 MIBs and updated in RFC 4293 to cover all IP management
- RFC 4295, Mobile IP Management MIB SHOULD+ be supported for Network Management in MIPv6 environment
- RFC 4807, IPsec Security Policy Database Configuration MIB SHOULD be supported when the IPsec Security Policy Database is used
- RFC 4292, IP Forwarding Table MIB SHOULD be supported

SNMP SHOULD+ be transported over IPv6; currently an IPv4 interface is permitted.

2.8 Routing Protocol Requirements

A Router may be deployed as an Exterior Router (at the network edge) or an Interior Router (in the network core). Router products MAY include both capabilities.

2.8.1 Interior Router Requirements

An Interior Router MUST support RFC 2740, OSPF for IPv6 (OSPFv3)[16]. Conditionally, an Interior Router implementing OSPFv3 MUST support RFC 4552, Authentication/Confidentiality for OSPFv3. An Interior Router MAY support other routing protocols as appropriate to the deployed routing architecture.

2.8.2 Exterior Router Requirements

An Exterior Router (BGP gateway) between routing systems MUST support:

- RFC 4271, A Border Gateway Protocol 4 (BGP-4)
- RFC 1772, Application of the Border Gateway Protocol in the Internet
- RFC 2545, Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing
- RFC 2858[17], Multi-protocol Extensions for BGP-4

2.9 Automatic Configuration

IPv6 includes two methods by which a node can automatically discover and configure its own unique global IPv6 interface address(es) along with other network configuration parameters. Stateless Address Autoconfiguration (SLAAC) and Dynamic Host Configuration Protocol for IPv6 (DHCPv6) are complementary methods, but not mutually exclusive. A product may include an implementation of either or both.

SLAAC is appropriate in deployments where Host/Workstation and Network Appliance nodes are permitted to obtain their interface address(es) dynamically from the currently available on-link router. DHCPv6 provides for a stateful equivalent to SLAAC in deployments where more central control is necessary, through administration of DHCP servers.

There will be deployments where static IP addresses are always assigned so all nodes implementing either or both autoconfiguration methods MUST have a configuration option to disable the autoconfiguration. Autoconfiguration is generally inappropriate for Intermediate Nodes (Routers, L3 Switches and IA Devices) and Servers but MAY be implemented for configuring the global addresses for administrative interface on any node. However, all nodes MUST generate link-local addresses as specified in RFC 4862 (replaces RFC 2462 as of version 3.0 of this document).

[16] An Internet Draft is currently on track in the OSPF Working Group to replace RFC 2740. See http://tools.ietf.org/html/draft-ietf-ospf-ospfv3-update-21

[17] Recently obsoleted by RFC 4760

2.9.1 Stateless Address Autoconfiguration (SLAAC)

An IPv6 Node using SLAAC to configure its unique IPv6 interface addresses MUST implement the host requirements specified by RFC 4862 (replaces RFC 2462 as of version 3.0 of this document) and SHOULD+ implement RFC 5175[18] extensions to Router Advertisement flags.

2.9.2 Dynamic Host Configuration Protocol – Version 6 (DHCPv6) Client

An IPv6 Node using DHCPv6 to configure its unique IPv6 interface address(es) MUST implement the client requirements specified by RFC 3315, DHCPv6.

2.9.3 DHCPv6 Server

An IPv6 Node that is deployed as a DHCPv6 Server MUST implement the server requirements specified by RFC 3315, DHCPv6 and SHOULD implement IPv6 Prefix Delegation as specified by RFC 3769 and RFC 3633.

2.9.4 DHCPv6 Relay Agent

An IPv6 Node that is deployed as a DHCPv6 Relay Agent MUST implement the relay agent requirements specified by RFC 3315, DHCPv6.

3 Product Class Profiles

The Product Class Profiles for each of the Product Classes defined in section 1.6 can now be specified in terms of the Functional Requirements defined in Section 2. For a specific product presented for evaluation as IPv6 Capable, the information in Section 1.6 should be used to determine the appropriate Product Class for the product and the corresponding Product Class Profile in the following sections.

Additional Product Classes may be added in the future as new products are developed and presented for evaluation, or these Product Classes may be modified to cover additional products. The following paragraphs provide detailed Profiles for each Product Class.

3.1 IPv6 End Nodes

3.1.1 Host/Workstation Product Class Profile

IPv6 Capable Host/Workstation Products:

- MUST implement the Base Requirements (Section 2.1);

[18] RFC 5175 obsoleted RFC 5075 which was cited in draft 2.1 of this document

- MUST implement RFC 3810, MLDv2;
- MUST implement at least one method of autoconfiguration, ether SLAAC as specified in section 2.9.1 or DHCPv6 autoconfiguration as specified in section 2.9.2;
- MUST be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);
    - And SHOULD+ support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Autoconfiguration;
    - Conditionally, Hosts/Workstations that will operate on networks requiring privacy address extensions or otherwise need to maintain anonymity MUST follow RFC 4941 (replaces RFC 3041) when generating interface identifiers;
- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;
- MAY support QoS Functional Requirements (Section 2.4);
- Conditionally, MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4) IF intended deployment requires interoperation with MIPv6 Capable Nodes;
- Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node;
- MUST implement Standard 66/RFC 3986, Uniform Resource Identifier (URI): Generic Syntax;
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default “policy table” and encourages implementations to allow manual configuration. Host/Workstation nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations).[19]

3.1.2 Network Appliance Product Class Profile

IPv6 Capable Network Appliances:

- MUST implement the Base Requirements (Section 2.1);
- SHOULD+ be IPsec Capable by supporting the IPsec Functional Requirements (Section 2.2);
- SHOULD support the complete Host/Workstation profile if possible.

[19] This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

While it is preferable that all IPv6 Capable Products interoperate with IPv4-Only legacy nodes and networks, a Network Appliance MAY be IPv6-Only and therefore rely upon external methods (tunneling or translation) to interoperate with IPv4.

3.1.3 Server Product Class Profiles

3.1.3.1 Advanced Server Profile

IPv6 Capable Advanced Servers:

- MUST implement the Base Requirements (Section 2.1);
  - And MUST implement RFC 3810, MLDv2;
- MUST be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);
- Conditionally, IF an Advanced Server is acting as a client AND needs to maintain anonymity, it MUST support RFC 4941 (replaces RFC 3041), Privacy Extensions for Stateless Address Autoconfiguration when generating interface identifiers; note that a server's primary address will likely be registered in DNS or well-known, so privacy addressing normally would not apply.
- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;
- MAY support QoS Functional Requirements (Section 2.4);
- Conditionally, MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4) IF intended deployment requires interoperation with MIPv6 Capable Nodes;
- MUST implement Standard 66/RFC 3986, Uniform Resource Identifier (URI): Generic Syntax;
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default "policy table" and encourages implementations to allow manual configuration. Advanced Server nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations).[20]

A Server will add services according to the manufacturer's service profile and the deployment requirements for the Server. The full service profile of applications offered by an advanced server is beyond the scope of this document, but should be available from the operating system manufacturer or by referencing industry standard profiles

[20] This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

such as the UNIX 03 Standard[21] Linux Base Standard (LSB)[22] or others. Whatever service profile is specified, the IPv6 Advanced Server is expected to offer an IPv6 equivalent of any IPv4 service that the Server is hosting, as well as any IPv6-only services specified in its service profile.

There are many network application services possible, a partial list of services that MAY be provided by a Server include:

- RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI[23]
- RFC 3596, DNS Extensions to Support IPv6
- RFC 3226, DNS Security and IPv6 Aware Server/Resolver Message Size Requirements
- RFC 3261, Session Initiation Protocol (SIP)
- Section 2.9.3 Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Server
- Section 2.9.4 DHCPv6 Relay Agent
- RFC 3053, IPv6 Tunnel Broker
- RFC 3162, RADIUS (Remote Authentication Dial In User Service) and IPv6
- RFC 2911, Internet Printing Protocol (IPP)
- RFC 2821, Simple Mail Transfer Protocol (SMTP)
- RFC 2428, FTP Extensions for IPv6 and NATs; Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands
- Standard 9/RFC 959, File Transfer Protocol (FTP)

3.1.3.2 Simple Server Profile

Requirements for IPv6 Capable Simple Servers are identical to Network Appliance, with the addition that a Simple Server :

- SHOULD meet the Advanced Server Profile if possible (section 3.1.3.1);
- SHOULD provide at least one network service as discussed in Section 3.1.3.1.

3.2 IPv6 Intermediate Nodes

3.2.1 Router Product Profile

IPv6 Capable Routers:

- MUST implement the Base Requirements (Section 2.1)
  - And MUST implement RFC 3810, MLDv2;

[21] http://www.opengroup.org/openbrand/register/xy.htm
[22] http://www.opengroup.org/lsb/cert/register.html

[23] A protocol specification draft for NTPv4 is on track for publication in the NTP working group. See http://tools.ietf.org/html/draft-ietf-ntp-ntpv4-proto-09

- MUST implement the router requirements defined in RFC 4862 (replaces RFC 2462 as of Version 3.0 of this document) including configuration of link-local addresses;
- MUST be IPsec capable, implementing the IPsec Functional Requirements (Section 2.2)
  - And SHOULD+ support RFC 4941 (replaces RFC 3041), Privacy Extensions;
  - And Conditionally, IF the Open Shortest Path First (OSPF) routing protocol is used the router MUST support RFC 4302 (AH) to secure OSPF;[24]
- MUST, at a minimum, support transport of both IPv4 and IPv6 traffic via Dual Stack OR manual tunneling Transition Mechanisms (Section 2.3)
- Conditionally, an edge router MUST support RFC 2784, Generic Router Encapsulation (GRE): IPv6-in-IPv4 tunnels when transiting IPv4 core network;
- Conditionally, an edge router MUST support RFC 2473, Generic Packet Tunneling in IPv6 Specification to provide IPv4-in-IPv6 tunnels;
- MUST support the QoS Functional Requirements (Section 2.4)
- Conditionally, A Router MUST implement Home Agent capability as defined in Section 2.5.2 IF it will be deployed as a Home Agent Router;
- Conditionally, A Router MUST implement MIPv6 Network Mobility (NEMO) capability as defined in Section 2.5.3 IF it will be deployed as a NEMO Capable Router.
- MUST support the Network Management Functional Requirements (Section 2.7)
- Conditionally, IF the router functions as an Interior Router (network core) it MUST support the Interior Router Requirements (Section 2.8.1)
- Conditionally, IF the router functions as an Exterior Router (BGP gateway) between routing systems, it MUST support the Exterior Router Requirements (Section 2.8.2)
- Conditionally, IF the Router functions as a DHCPv6 Server it MUST implement Section 2.9.3.
- Conditionally, IF the Router functions as a DHCPv6 Relay Agent it MUST implement Section 2.9.4.

A Router product MAY implement one or more Information Assurance functions as defined in section 3.2.3. As such, the router would be an “IA Enabled Product”.

Note on multicast routing protocols: Multicast routing protocols have recently emerged from the IETF Protocol Independent Multicast (PIM) Working Group as

[24] This is to be consistent with the DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG) which states the following: "(BTS-RTR-010: CAT II) The router administrator will ensure neighbor authentication with MD5 or *IPv6 AH is implemented for all routing protocols* with all peering routers within the same autonomous system as well as between autonomous systems." Implementing IPsec to secure routing protocols would make a router an “IA Enabled Device” rather than an “IA Device”.

Proposed Standards. RFC 4601, Protocol Independent Multicast – Sparse Mode (PIM-SM) and RFC 3973, Protocol Independent Multicast – Dense Mode (PIM-DM) conditionally **SHOULD+** be implemented IF deployment requires multicast routing protocols.

3.2.2 Layer-3 (L3) Switch Product Profile

IPv6 Capable L3 Switches:

- MUST implement the Base Requirements (Section 2.1)
- SHOULD+ be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2)
- Conditionally, IF the L3 Switch is used as an Exterior Router it
    - MUST support the Exterior Router Requirements (Section 2.8.2) IF the product will be used as an exterior system node and must support routing functions to interface with routers at edge of a switching network
    - MUST, at a minimum, support transport of both IPv4 and IPv6 traffic via Dual Stack OR manual tunneling Transition Mechanisms (Section 2.3)
- Conditionally, IF the L3 Switch is used as an Interior Router it MUST support the Interior Routing Requirements (Section 2.8.1)
- Conditionally, MUST support the Network Management Functional Requirements (Section 2.7) IF the product is a managed switch
- Conditionally, SHOULD support RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches IF MLD Snooping is required in the deployment;
- MUST implement the “multicast router” requirements and the “multicast address listener” part of RFC 2710 and conditionally, IF RFC 3810 is supported, MUST implement the “multicast router” requirements and the “multicast address listener” part of RFC 3810.

A L3 Switch product MAY implement one or more Information Assurance functions as defined in section 3.2.3. As such, the router would be an “IA Enabled Product”.

3.2.3 Information Assurance (IA) Device Product Profile

An IPv6 Capable Information Assurance (IA) Device provides one or more Information Assurance functions:

- Intrusion Detection
- Intrusion Protection
- Firewall
- Security Proxy
- In-line Network Encryptor (INE)
- Virtual Private Network (VPN) server
- VPN remote access client software
- Authentication, Authorization and Accounting (AAA) server

This specification only addresses the requirements for an IPv6 Capable IA Device to interoperate in an IPv6 environment; the specific IA function is beyond the scope of these requirements, and beyond the scope of testing based on this specification. Previously established policies and requirements already cover the evaluation and approval of several types of IA devices. The IPv6 Capable evaluation process does not affect or change the requirements defined by the National Information Assurance Partnership (NIAP) or FIPS 140-2 or any other mandated requirements on Information Assurance Devices. Specific guidance on IA can be found in the memorandum Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objective 2 (MO2) Version 1.1 [12] and MO3 to follow.

In addition to its IA functions, An IPv6 Capable IA Device is a “middlebox” and may be viewed as an IPv6 Capable Intermediate Node, forwarding (or blocking) packets depending on the security policy it is implementing. The IA Device will present one or more IPv6 interfaces to the network, and therefore can be evaluated for IPv6 interoperability on those interfaces. The device may behave like an end-node on the network side while appearing to be a router on the LAN side. An IA Device may not participate in all IPv6 support protocols, by the nature of the architectural role it plays. Some IA Devices (for example an Intrusion Detection System) may need to maintain transparency to protocols such as Neighbor Discovery, ICMPv6, IPsec, etc. to perform their mission. Therefore it is not straightforward to specify how such a device can be IPv6 Capable, and it is challenging to verify compliance through testing.

Regardless of how the device is evaluated on its data path, an IA Device may also operate as an IPv6 Capable end-node to be managed via its User Interface or SNMP.

IPv6 Capable IA Devices:

- MUST implement the Base Requirements (Section 2.1)
- Conditionally, MUST be IPsec Capable, implement the IPsec Functional Requirements, IF the device is an IPsec based in-line network encryptor (INE), VPN server, or if it must exchange information with other devices across IPsec secured connections. Some instances of intrusion detection devices, simple firewalls, and other security devices may simply monitor traffic flows and not actually send/receive data across the network and may not require IPsec.
- These devices SHOULD+ support the complete IPsec Functional Requirements but MAY support the following minimal subset of the IPsec requirements:
    - RFC 4301, Security Architecture for the Internet Protocol
    - RFC 4303, IP Encapsulating Security Payload (ESP)
    - Manual Keying
- If a security device must distribute IP Security Policy information to other devices, it SHOULD+ implement:
    - RFC 3585, IPsec Configuration Policy Information Model
    - RFC 3586, IP Security Policy Requirements

  - Note: New Security device standards are emerging for managing IPsec policy information, managing distributed firewalls, etc., which will fit in this category. There is no official DoD IPv6 IPsec policy available at this time.
- Devices MUST also support IPv6 requirements defined for any special security function of the device. Example:
  - Conditionally, Remote Authentication Dial In User Service (RADIUS) authentication servers MUST support RFC 3162, Remote Authentication Dial In User Service (RADIUS) and IPv6, when used to support IPv6 networks.

3.2.3.1 Integrated Security Device (ISD) Additional Requirements

An Integrated Security Device (ISD) is a device that performs stateful packet inspection of both the IPv4 and IPv6 protocols and performs Intrusion Prevention and Intrusion Detection functions (IPS/IDS) within the same device on both IPv4 and IPv6 protocol stacks. An IPv6 Capable ISD MUST support the Information Assurance Device Profile requirements.

3.2.3.2 IPv6 Security Proxy Additional Requirements

An IPv6 Security Proxy is a device or appliance that is designed to terminate a session and initiate a session on the behalf of an IPv6 host. An IPv6 Security Proxy also serves as a network segregator for services and applications. A Security Proxy Appliance has a scalable proxy platform architecture to secure Web communications and accelerate delivery of business applications.

- An IPv6 Security Proxy MUST support the Information Assurance Device Profile Requirements.
- An IPv6 Security Proxy is limited to Tunnel Mode IPsec, and MUST NOT provide Transport Mode IPsec.

3.2.3.3 HAIPE Devices

The High Assurance IP Encryption device (HAIPE) is a special case of IA Device. The HAIPE is designed for pair-wise deployment, providing peer-to-peer implementation of encryption using IPsec (in particular, ESPv3 transport mode and IKEv2) to protect classified traffic over an open network. The HAIPE is a “bump-in-the-wire” device; on one side, the plaintext or PT interface connects to host/workstation device or LAN; on the other side, the cypertext or CT interface connects to an IPv6 backbone network. The HAIPE presents a unique problem to testing:

a. As a cryptographic device, the HAIPE has its own set of specifications and requirements [15] and test plans and must be certified by a designated test facility at the Space and Naval Warfare Systems Command (SPAWAR);
b. As an IPv6 Capable device, the CT side SHOULD+ meet the requirements of this specification for a Host/Workstation, and the PT side SHOULD+ meet the requirements for a Router;

c. Where requirements are inconsistent or in conflict, the HAIPE specifications and test plans take precedence over this specification; the authors are not aware of any conflicts that would interfere with the interoperability of approved HAIPE devices with other IPv6 Capable products that comply with this specification.

3.2.3.4 IPv6 Firewalls

Like HAIPE, firewalls are covered by established policies for test and evaluation. By their nature, firewalls intentionally interfere with standard protocols by blocking the transit of packets that are permitted by the specification but are forbidden by other security requirements. A good example is the IPv6 Routing extension header type 0 (RH0) which allows a sender (or an attacker) to dictate intermediate nodes in the routing of the packet and any response. As with IPv4 source routing, a firewall may be configured to block IPv6 packets with RH0 to prevent the attack scenario. Although RH0 has been deprecated by RFC 5095, there may still be products that generate or respond to RH0 and a firewall configured to block RH0 would ensure that this vector cannot be used.

The National Security Agency (NSA) has a publication “Firewall Design Considerations for IPv6” [18] which explains the role of a firewall in an IPv6 network. This document includes analysis of the IPv6 implications of IPsec, tunneling, higher layer protocols and other topics on firewall design and operation. Current requirements and testing procedures defined under Common Criteria do not address IPv6, but we anticipate that NSA will develop and publish procedures for IPv6 firewalls. NSA public information can be found at http://www.nsa.gov/ as well as the Common Criteria site http://www.niap-ccevs.org/cc-scheme/.

4 IPv6 Capable Software

We anticipate that software products will be presented for evaluation as IPv6 Capable, but the specific requirements for IPv6 Capable software are limited. Further analysis is needed to develop Product Class definitions for software products, but this section is included to document the current state of the discussion on requirements for Software products.

Software products can be divided into Operating System products, Middleware and Application products, with the following definitions:

Operating System (OS): The foundational software on a Host/Workstation or Server that provides an environment for running applications. The OS includes the communications software (drivers) that provide the IPv6 capabilities and an Application Programming Interface (API) that allows IPv6 Capable Applications to use these features.

Middleware: Middleware is software that provides a layer of functionality between the OS and application software, or between the hardware platform and the OS. An example of the former would be a relational database management system (RDBMS) that can be used to build various applications, while an example of the latter would be a virtualization product that enables running multiple instances of one or more operating systems on the same platform.

Application: Software expressing specific functional requirements, particular to its use. The evaluation of an Application software product as IPv6 Capable is based on its use of IPv6 addresses and other IPv6-specific features available through the API.

Application Vendors can be expected to scan and test their code for IPv6 compliance and provide a letter of compliance indicating to what degree they comply. End users of Applications will be looking to DISA to verify that the Application will interoperate with other IPv6 components based on the DISR profiles. Third party or packaged Applications may be considered COTS if they have already been submitted by the vendor, tested and on the IPv6 Capable Registry. Embedded or custom applications as well as unevaluated vendor Applications (i.e. not on the Registry) will be subject to testing.

General purpose Operating Systems can be considered COTS components, if previously submitted by the vendor, tested, and on the APL. This will limit the scope of testing to verifying IPv6 compliance of IPv6-specific requirements upon the application itself in these cases. In cases where the Application under test includes a proprietary or customized Operating System, the test plan may also address the IPv6 functional requirements on the operating system.

An Application or Operating System cannot be tested in isolation; some level of integration testing will be achieved when exercising the two components. Novel combinations of previously approved COTS Applications and Operating Systems may be subjected to Integration Testing, but in general that would be an end-user responsibility.

4.1 Application Programming Interface (API) Characteristics

All applications on Hosts/Workstations, Advanced Servers, Simple Servers or Network Appliances that require IP network protocol service MUST use IPv6 Capable versions of those network protocols. These include the basic and extended specifications of the Socket API as appropriate to the application architecture[25]. Applications will require evaluation and testing for approval as IPv6 capable as components of a system under test (embedded software) or as a stand-alone product.

Currently, generic requirements are not defined for an IPv6 Capable application beyond the following:

[25] The Socket API extensions are defined in Informational RFCs, as they would not apply to all applications, i.e. those that use other operating system methods for networking.

- IEEE Standard 1003.1-2001, based on The Open Group's Networking Services (XNS) specification, issue 5.2; RFC 3493, Basic Socket Interface Extensions for IPv6 is an informational recap of this specification
- RFC 3542, Advanced Sockets Application Program Interface (API) for IPv6
- RFC 4038, Application Aspects of IPv6 Transition
- On MIPv6 Capable Nodes, for some Mobile applications, RFC 4584, Extension to Sockets API for Mobile IPv6
- RFC 5014, IPv6 Socket API for Source Address Selection is an emerging specification

In addition, specific requirements may be needed for various classes of applications including:

1. File Transfer Protocol (FTP) client

2. Web Browser

3. E-mail client

4. IM client

It is also suggested that applications comply with RFC 3986 Uniform Resource Identifiers: Generic Syntax, for the representation of IPv6 addresses in user interfaces.

4.2 Software Requirements

An IPv6 Capable Application software product will be evaluated on its ability to send and receive IPv6 packets with an IPv6 client, and its use of IPv6 addresses and features available through the API.

IPv6 Capable Operating Systems Conditionally MUST support Dual Stack and MUST support both IPv4 and IPv6 applications in the Application Program Interface (APIs) when deployed with IPv4 legacy peers.

Appendix A: References

The primary source for requirements cited in this document is the body of Internet Engineering Task Force (IETF) specifications known as "Request For Comment" (RFC) which are referenced throughout the document. These references can be found through http://www.ietf.org/ by using the RFC Search feature on the RFC Editor page. The Requirements Summary Table (Appendix C) can be used as a cross-reference for the RFCs cited as requirements in this document.

The following additional sources were used in generating requirements for this document:

[1] "Internet Protocol Version 6 (IPv6) Interim Transition Guidance" John Stenbit, CIO U.S. Department of Defense; September 23, 2003

[2] "Internet Protocol Version 6 (IPv6)" DoD CIO Memorandum; June 9, 2003

[3] DoD Information Technology Standards Registry (DISR); a repository of cited standards to be followed by DoD projects and deployments. This database can be accessed by authorized users via the web at https://disronline.disa.mil/

[4] "Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Draft IPv6 Capable Functional Specification v1.0" November 22 2005

[5] "Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Solutions Version 1.0" September 8, 2005

[6] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 06-02; June 27, 2006. This Memorandum linked Version 1.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products

[7] NIST Communications Security Establishment document "FAQ for the Cryptographic Module Validation Program" updated December 8, 2006 http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf

[8] Memorandum for Secretaries of the Military Departments, et al "Internet Protocol Version 6 (IPv6) Policy Update" issued by Assistant Secretary of Defense – Networks and Information Integration, August 16, 2005

[9] NIST Special Publication 500-267 "A Profile for IPv6 in the U.S. Government – Version 1.0" draft for public comment, February 22, 2007

[10] Internet Draft “Deprecation of Type 0 Routing Headers in IPv6” J. Abley et al, May 16, 2007; this is a work in progress, which will update RFC 2460 if approved.

[11] “The Teredo Protocol: Tunneling Past Network Security and Other Security Implications” Dr. James Hoagland, Symantec Report http://www.symantec.com/avcenter/reference/Teredo_Security.pdf

[12] Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objective 2 (MO2) Version 1.1

[13] DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG) http://iase.disa.mil/stigs/index.html

[14] The Department of Defense Internet Protocol Version 6 Address Plan – version 1.0; Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer; March 2008

[15] High Assurance Internet Protocol Encryptor Interoperability Specification Guide: HAIPE IS version 3.1.2; National Security Agency; 29 February 2008

[16] IEEE 802.11-2007 Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE 3 Park Ave, NYC NY 12June 2007 http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[17] IEEE 802.11i Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements, IEEE 3 Park Ave, NYC NY 12June 2007 http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[18] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 07-03; 6 November 2007. This Memorandum linked Version 2.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products. We anticipate that a similar Memorandum will be issued when Version 3.0 is approved.

[19] NIST Special Publication 500-267 “A Profile for IPv6 in the U.S. Government – Version 1.0 Draft 2” draft for public comment, 23 January 2008

Appendix B: Glossary

This glossary is provided for the convenience of the reader, and is intended to include terminology and acronym definitions specific to this document, plus other terms in general use.

Information Assurance Device: An Intermediate Node that performs a security function as its primary purpose by filtering or encrypting network traffic, and which may block traffic when security policy dictates. For example a Firewall, Intrusion Detection System, Authentication Server, Security Gateway, HAIPE or VPN are Information Assurance Devices.

Information Assurance Enabled: An IPv6 Capable Node may incorporate an IA function in addition to its primary role, for example implementing cryptographic algorithms as part of IPsec protocols. This is not the core role of the device so it should not be considered an IA Device but rather is an "IA Enabled" product.

IP: Internet Protocol; the glue that holds the Internet together, that is the network layer protocol for the interconnection of packet-switched networks. The first widely deployed version of IP was IP version 4, defined and implemented over 25 years ago.

IPv6: The Internet Protocol Version 6; a replacement for the widely deployed Internet Protocol Version 4. IPv6 and related protocols are defined by IETF in RFCs which can be found at http://www.ietf.org/. Basic information on IPv6 can be found at http://en.wikipedia.org/wiki/IPv6 or through the North American IPv6 Task Force.

IETF: The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. More information can be found at http://www.ietf.org/.

RFC: Request for Comment; for historical reasons, publications of the IETF are called Requests for Comment, but everyone just calls them RFCs. When an Internet-Draft is accepted for publication, the RFC Editor assigns a number which permanently identifies the publication. Thus any RFC cited can be found by number through the RFC Editor.

IPv6 Capable: According to the IPv6 Interim Transition Memorandum [1] an "IPv6 Capable" system or product shall be capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other protocols in a manner similar to IPv4. Specific criteria for determining whether a product is an IPv6 Capable Product is defined by this document.

IPv6 Capable Product: The term "IPv6 Capable Product" as used in this document, is any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Thus an IPv6 Capable Product is one that meets the IPv6 Capable requirements specific to the Product Profile for the Product Class appropriate for the product.

Product Class: as used in this document a Product Class is one of a set of definitions used in this document to group products with common characteristics and requirements.

SLAAC: Stateless Address Autoconfiguration; one of the methods of configuring end-node interface addresses for IPv6, relying on Neighbor Discovery Protocol (NDP) and Duplicate Address Detection (DAD) to construct globally unique addresses using network prefixes assigned and advertised by a router.

Appendix C: Requirements Summary Table

The Requirements Summary Table list RFC numbers and notes on their applicability to each Product Class.

RFC Status: Info – Informational; PS – Proposed Standard; DS – Draft Standard; STD – Approved Standard; BCP – Best Current Practice; OBS – Obsolete; HIST – Historic; EXP – Experimental

Applicability: M – MUST; S+ – SHOULD+; S – SHOULD; O – Optional (MAY); C – Conditional (followed by another code, for example C M indicates Conditional MUST); I – Informational; SN – SHOULD NOT; MN – MUST NOT

In-effect Date: Date at which the requirement will be in effect for products; "current" indicates requirements already in effect as of this publication

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
2.1	Base Requirements	2460	Internet Protocol, Version 6 (IPv6) Protocol Specification	DS	M	M	M	M	M	M	Current
		5095	Deprecation of Type 0 Routing Headers in IPv6	PS	M	M	M	M	M	M	7/2009
		4443	Internet Control Message Protocol (ICMPv6)	DS	M	M	M	M	M	M	Current
		4861 [replaces 2461]	Neighbor Discovery for IPv6	DS	M	M	M	M	M	M	7/2009 [2461 Current]

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4862 [replaces 2462]	IPv6 Stateless Address Autoconfiguration [only link-local addresses and Duplicate Address Detection]	DS	M	M	M	M	M	M	7/2009 [2462 Current]
		1981	Path MTU Discovery for IPv6	DS	M	S	M	M	M	M	Current
	[address architecture]	4291	IPv6 Addressing Architecture	DS	M	M	M	M	M	M	Current
		4007	Scoped Address Architecture	PS	M	M	M	M	M	M	Current
		4193	Unique Local IPv6 Unicast Addresses	PS	O	O	O	O	O	O	Current
	[Multicast listener discovery]	2710	Multicast Listener Discovery for IPv6	PS	M	M	M	M	M	M	Current
		3810	MLDv2 for IPv6	PS	M	S+	M	M	S+[26]	S+	Current
	[connection technology]	2464	IPv6 over Ethernet	PS	C M	C M	C M	C M	C M	C M	Current
		2492	IPv6 over ATM	PS	C M	C M	C M	C M	C M	C M	Current
		5072 [replaces 2472]	IPv6 over PPP	PS	C M	C M	C M	C M	C M	C M	7/2009 [2472 Current]
		3572	IPv6 over MAPOS	PS	C M	C M	C M	C M	C M	C M	Current

[26] Note that an L3 Switch MUST also implement the “multicast router part” and “multicast address listener part” of RFC 3810 IF supporting RFC 3810.

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		2467	IPv6 over FDDI	PS	C M	C M	C M	C M	C M	C M	Current
		2491	IPv6 over NBMA	PS	C M	C M	C M	C M	C M	C M	Current
		2497	IPv6 over ARCnet	PS	C M	C M	C M	C M	C M	C M	Current
		2590	IPv6 over Frame Relay	PS	C M	C M	C M	C M	C M	C M	Current
		3146	IPv6 over IEEE 1394 Networks	PS	C M	C M	C M	C M	C M	C M	Current
		4338	IPv6, IPv4 and ARP Packets over Fibre Channel	PS	C M	C M	C M	C M	C M	C M	Current
		4944	Transmission of IPv6 Packets Over IEEE 802.15.4 Networks	PS	C M	C M	C M	C M	C M	C M	7/2009
2.2	IPsec	4301	Security Architecture for the Internet Protocol	PS	M	S+	M	M	S+	C M	Current
		4302	IP Authentication Header	PS	S	S	S	C M	S	C S	Current
		4303	IP Encapsulating Security Payload	PS	M	S+	M	M	S+	C M	Current
		4308 [VPN-B]	Cryptographic Suites for IPsec	PS	M	S+	M	M	S+	C M	7/2009

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4835 [replaces 4305]	Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)	PS	M	S+	M	M	S+	C M	7/2009 [4305 Current]
		4869	Suite B Cryptographic Suites for IPsec	Info	M	S+	M	M	S+	C M	7/2009
		IEEE 802.11-2007i	Standard for Information Technology Part 11 – Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment 6 MAC Security Enhancements	PS	C S	C S	C S	C S	C S	C S	Current
	IPsec Fallback[27]	2401	Security Architecture for the Internet Protocol	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2406	IPsec Encapsulating Security Payload (ESP)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2402	IPsec Authenticating Header (AH)	OBS	C M	C S+	C M	C M	C S+	C M	Current
	[SeND]	3971	Secure Neighbor Discovery	PS	S	S	S	S	S	S	Current

[27] IPsec Fallback requirements only apply to a product that MUST support IPsec that does not currently support IPsec RFC 4301 requirements

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
	[CGA]	3972	Cryptographically Generated Addresses	PS	S	S	S	S	S	S	Current
	[SLAAC Privacy Extension]	4941 [replaced 3041]	Privacy Extensions for Stateless Address Auto configuration in IPv6	PS	S+ C M	S	C M	S+	S	S	7/2009 [3041 Current]
2.2.2	IKEv2	4306	Internet Key Exchange Version 2 (IKEv2) Protocol	PS	M	S+	M	M	S+	C M	7/2010
		4307	Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2)	PS	M	S+	M	M	S+	C M	7/2010
	IKEv1[28]	2407	The Internet IP Security Domain of Interpretation for ISAKMP	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2408	Internet Security Association and Key Management Protocol (ISAKMP)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		2409	The Internet Key Exchange (IKE)	OBS	C M	C S+	C M	C M	C S+	C M	Current
		4109	Algorithms for Internet Key Exchange Version 1 (IKEv1)	PS	C M	C S+	C M	C M	C S+	C M	Current

[28] Products with IKEv2 implementation MAY also include a fall-back to IKEv1; products without IKEv2 MUST at least meet the IKEv1 requirements

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4304	Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)	PS	C S	C S	C S	C S	C S	C S	7/2009
2.3	Transition Mechanisms	4213	Transition Mechanisms for IPv6 Hosts and Routers [Dual Stack]	PS	C M[29]	S	C M[29]	M[29]	C M[29]	S	Current
		4213	Transition Mechanisms for IPv6 Hosts and Routers [manual tunnels]	PS							Current
		4213	Transition Mechanisms for IPv6 Hosts and Routers [Translation and other methods]	PS	O	O	O	O	O	O	Current
		2766	Network Address Translation – Protocol Translation (NAT-PT)	PS (HIST)	SN	SN	SN	SN	SN	SN	Current
		3053	IPv6 Tunnel Broker	INFO	C M	C S	C M	C M	C M		Current
	[provider edge]	4798	Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers	PS				C S	C S		Current

[29] MUST implement Dual Stack OR Tunneling to meet the requirement to carry both IPv4 and IPv6 traffic

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
2.4	QoS	2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers	PS	O	O	O	M	O		Current
		3168	The Addition of Explicit Congestion Notification (ECN) to IP	PS	O	O	O	S	O		Current
		2205	Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification	PS	O	O	O	S+	O		Current
		2207	RSVP Extensions for IPSEC Data Flows	PS	O	O	O	S+	O		Current
		2210	The Use of RSVP with IETF Integrated Services	PS	O	O	O	S+	O		Current
		2750	RSVP Extensions for Policy Control	PS	O	O	O	S+	O		Current
		3175	Aggregation of RSVP for IPv4 and IPv6 Reservations	PS	O	O	O	O	O		Current
		3181	Signaled Preemption Priority Policy Object	PS	O	O	O	O	O		Current
		2961	RSVP Refresh Overhead Reduction Extension	PS	O	O	O	O	O		Current
		4495	A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow	PS	O	O	O	O	O		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		2998	A Framework for Integrated Services Operation over DiffServ Networks	I	O	O	O	O	O		Current
		2996	Format of the RSVP DCLASS Object,	PS	O	O	O	O	O		Current
		2746	RSVP Operation Over IP Tunnels	PS	O	O	O	O	O		Current
		3182	Identity Representation for RSVP	PS	O	O	O	O	O		Current
		2872	Application and Sub Application Identity Policy Element for Use with RSVP	PS	O	O	O	O	O		Current
		2747	RSVP Cryptographic Authentication	PS	O	O	O	O	O		Current
2.5.1	MIPv6 Capable	3775 [Mobile Node]	Mobility Support in IPv6	PS	C M	C S					Current
		3776	Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents	PS	C M	C S					Current
		4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	PS	C M	C S					7/2010
		4282	The Network Access Identifier	PS	C S+	C S					Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4283	Mobile Node Identifier for Option for IPv6	PS	C S+	C S					Current
2.5.2	Home Agent Router	3775 [Home Agent]	Mobility Support in IPv6	PS				C M			Current
		3776	Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents	PS				C M			Current
		4877	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	PS				C M			7/2010
		4282	The Network Access Identifier	PS				C S+			Current
		4283	Mobile Node Identifier for Option for IPv6	PS				C S+			Current
2.5.3	NEMO Capable	3963	Network Mobility (NEMO) Basic Support Protocol	PS				C M			Current
2.5.4	Route Optimization	3775 (sect 9)	Mobility Support in IPv6	PS	C M	C S	C M				Current
2.6.1	RoHC	3095	Robust Header Compression (RoHC)	PS	O	O	O	O	O		Current
		4815	Corrections and Clarifications to RFC 3095	PS	O	O	O	O	O		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4995	RoHC Framework	PS	O	O	O	O	O		Current
		4996	RoHC: A profile for TCP/IP	PS	O	O	O	O	O		Current
		3241	RoHC over PPP	PS	O	O	O	O	O		Current
		3843	RoHC: A Compression Profile for IP	PS	O	O	O	O	O		Current
		4362	RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP	PS	O	O	O	O	O		Current
2.6.2	IP Header Compression	2507	IP Header Compression	PS	O	O	O	O	O		Current
		2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	PS	O	O	O	O	O		Current
		3173	IP Payload Compression	PS	O	O	O	O	O		Current
2.7	Network Management	3411	An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3)	STD 62				M	C M		Current
		3412	Message Processing and Dispatching for the SNMP	STD 62				M	C M		Current
		3413	SNMP Applications	STD 62				M	C M		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
			SNMP over IPv6					S+	S+		7/2010
	[MIBs]	3595	Textual Conventions for IPv6 Flow Label	PS				M	C M		Current
		4022	Management Information Base for the Transmission Control Protocol	PS				M	C M		Current
		4113	Management Information Base for the User Datagram Protocol	PS				M	C M		Current
		4087	IP Tunnel MIB	PS				S	S		Current
		4293	Management Information Base (MIB) for IP	PS				M	C M		Current
		4295	Mobile IP Management MIB	PS				C M	C M		Current
		4807	IPsec Security Policy Database Configuration	PS				C M	C M		Current
		4292	IP Forwarding Table MIB	PS				M	C M		Current
	[Multicast]	4601	Protocol Independent Multicast – Sparse Mode (PIM-SM)	PS				C S+			Current
		3973	Protocol Independent Multicast – Dense Mode	PS				C S+			Current
2.8.1	Interior Router	2740	OSPF for IPv6 (OSPFv3)	PS				C M	C M		Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4552	Authentication/Confidentiality for OSPFv3	PS				C M	C M		Current
2.8.2	Exterior Router	4271	A Border Gate Protocol (BGP-4)	DS				C M	C M		Current
		1772	Application of the Border Gateway Protocol in the Internet	DS				C M	C M		Current
		2545	Use of BGP-4 Multi-Protocol Extensions for IPv6 Inter-Domain Routing	PS				C M	C M		Current
		4760 [replaces 2858]	Multi-Protocol Extensions for BGP-4	PS				C M	C M		7/2009 [2858 Current]
2.9	Automatic Configuration	4862 [replaces 2462]	IPv6 Stateless Address Auto-configuration (SLAAC)	DS	M[30]	M[30]		M[30]			7/2009 [2462 Current]
		3315	DHCPv6 [client]	PS							Current
		3315	DHCPv6 [server]	PS		C M	C M	C M			7/2009
		3315	DHCPv6 [Relay Agent]	PS				C M	C M		7/2009
		3769	IPv6 Prefix Delegation	PS		C M	C M	C M			7/2009

[30] Host and Net Appliance Product Classes MUST support a method of autonomous configuration, either SLAAC or DHCPv6 client; Routers MUST support Router requirements for SLAAC.

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		3633	IPv6 Prefix Options for DHCPv6	PS		C M	C M	C M			7/2009
		n/a	[disable autoconfiguration]		M	M	M	M	M	M	Current
		5175	Extensions to Router Advertisement Flags	PS	C S+	C S+	C S+	C S+	C S+	C S+	7/2009
3.1.3.1	Server [Services]	959	File Transfer Protocol	STD 9		O	O				Current
		2428	FTP Extensions for IPv6 and NAT	PS		O	O				Current
		2821	Simple Mail Transfer Protocol (SMTP)	PS		O	O				Current
		2911	Internet Printing Protocol	PS		O	O				Current
		3162	RADIUS (Remote Authentication Dial-In User Service) and IPv6	PS		O	O			C M	Current
		4330	Simple Network Time Protocol (SNTP)	INFO		O	O				Current
		3226	DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements	PS		O	O				Current
		3261	Session Initiation Protocol (SIP)	PS		O	O				Current
		3596	DNS Extensions to Support IPv6	DS		O	O				Current
		3053	IPv6 Tunnel Broker	INFO		O	O				Current

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
3.1.1	Host	3484 [Sec 2.1]	Default Address Selection for IPv6 [Policy Table]	PS	S+	S	S+				Current
		3484 [rest of RFC]	Default Address Selection for IPv6	PS	M	S	M				Current
		3596 [resolver]	DNS Extensions to Support IPv6	DS	M	S	M				Current
		3986	Uniform Resource Identifier (URI): Generic Syntax	STD 66	M	S	M				Current
3.2.1	Router	2784	Generic Router Encapsulation (GRE):	PS				C M			Current
		2473	Generic Packet Tunneling in IPv6	PS				C M			Current
3.2.2	L3 Switch	4541	Considerations for IGMP and MLD Snooping Switches	Info					C S		Current
3.2.3	IA Device	3585	IPsec Configuration Policy Information Model	PS						C S+	Current
		3586	IP Security Policy Requirements	PS						C S+	Current
4.1	API	3493	Basic Socket Interface Extensions for IPv6	INFO							
		3542	Advanced Sockets Application Program Interface for IPv6	INFO							

Functional Requirements Section		RFC			Applicability by Product Class						In-effect Date
Number	Title [sub-topic]	Number [note]	Title [sub-topic]	Status	Host	Net App or Simple Server	Adv Server	Router	L3 Switch	IA Device	
		4038	Application Aspects of IPv6 Transition	INFO							
		4584	Extension to Sockets API for Mobile IPv6	INFO							
		5014	IPv6 Socket API for Source Address Selection	INFO							
		3986	Uniform Resource Identifiers: Generic Syntax	STD 66							

Appendix D: Summary of Revisions from Version 2.0

This (draft) specification includes revisions based on comments received since the publication of Version 2.0, dated August 2007 and officially promulgated on 6 November 2007. Many of the comments were minor editorial and clarification points which have been addressed in the text; however, a number of substantive additions and revisions have been received and addressed in this version. The following tables highlight substantial changes as an aid to the reader in comparing Version 2.0 and Version 3.0.

Paragraph	Type of Edit	Change from v2.0 to v3.0
1.5.1	Addition	Based on several comments and requests, Version 3.0 defines a general policy for the timing of mandate for new or revised standards, and specific schedule notes for several requirements throughout the document
1.5.1, App C	Update	Allow 12-24 months (after this publication) for Effective Date window depending on requirement, rather than blanket 18 month as stated in v2.1; corresponding date changes in App C to 7/2009 or 7/2010
1.5.3	Addition	New text suggesting that test results indicate whether a particular product includes conditional requirements
1.6, 3.1	Update	Collapse Network Appliance and Simple Server to a single product class; but continue to use the two names and maintain section 3.1.3.2 for comparability to earlier version.
1.6	Clarification	Clarify that an operating system using a hardware implementation of the IPv6 stack embodies “IPv6 Capable” independent of the hardware platform, same as an OS that included the stack in software.
2.0	Addition	Per request of RTS program, added text explaining that programs may extend or modify requirements for specific circumstances in their own requirements documents.
2.1	Update	RFC 4861 replaces RFC 2461 as a mandatory standard as of Version 3.0 of this document and is preferred; products implementing RFC 2461 will be considered compliant until 31-December-2009

Paragraph	Type of Edit	Change from v2.0 to v3.0
2.1	Update	RFC 4862 replaces RFC 2462 as a mandatory standard as of Version 3.0 of this document and is preferred; products implementing RFC 2462 will be considered compliant until 31-December-2009
2.1	Addition	SHOULD+ RFC 3590 Source Address Selection for Multicast Listener
2.1	Deletion	Address Autoconfiguration is removed from Base Requirements; the requirement for Autoconfiguration no longer applies to all product classes
2.1	Clarification	Reword the statement on Autoconfiguration to clarify that portions of RFC 4862 apply to all nodes, specifically the MUST statements on Duplicate Address Detection and the automatic configuration of link-local addresses. Corresponding change in App C Base Requirements
2.2	Addition	Added clarifying language about the architectural role of nodes in IPsec and the use of other security tools
2.2	Update	RFC 4941 replaces RFC 3041 for Privacy Addressing, and the requirement is strengthened to a Conditional MUST; updated other references to 3041 throughout text and in Appendix C
2.2.1	Update	RFC 4869 strengthened to MUST
2.2.1	Update	Specify minimal requirement for interoperability as Suite-B-GCM-128 and Suite-B-GMAC-128
2.2.1	Update	Effective date for IPsec RFC 4301 architecture is stated as Current due to it being a MUST since version 1 publication
2.2.1	Update	Restore requirement for RFC 4308 removed in error in v2.0; clarify explanation of 4308 and 4869 and inclusion of the suites
2.2.2	Update	Relaxed statement on support for IKEv1 fall-back for interoperability; IKEv2 implementations MAY (but are not required to) implement IKEv1 as well.

Paragraph	Type of Edit	Change from v2.0 to v3.0
2.2.2	Update	Effective date for IKEv2 is July 2010, also implementations must include support for IKEv1 for interoperability; MUST on IKEv1 fall-back for IKEv2 implementations reduced to MAY
2.2.3	Addition	New section describing the fallback requirements for products that do not at this time meet the MUST requirements for IPsec RFC 4301 and IKEv2; at a minimum products Conditionally MUST support IPsec RFC 2401 and IKEv1. Corresponding changes inserted in App C.
2.3	Clarification	Clarify deprecation of Teredo, and reword the requirements
2.3	Correction	Text incorrectly cited RFC 3053 as MAY, should be Conditional MUST consistent with Appendix C
2.4	Addition	Cited several additional optional RFCs for QoS
2.5, 2.5.1, 2.5.2	Update	RFC 4877 updates 3776 for MIPv6 security
2.6.1	Addition	Add citation of RFCs 4815, 4995 and 4996
2.6.1, 2.6.2	Clarification	RoHC and IP Header compression are restated as “optional” to be consistent with Appendix C in v2.0
2.6.2	Addition	Add citation of RFC 3173
2.7	Addition	SNMP SHOULD+ be over IPv6; effective date +24 months
2.8.2	Update	RFC 4760 replaces RFC 2858
2.9	Addition	New section clarifying and elaborating on Autoconfiguration requirements
2.9.1	Addition	RFC 5075 extensions to Router Advertisement flags
2.9.1	Update	RFC 5175 obsoletes RFC 5075
3.1.1	Clarification	Reference to new section 2.9, clarifying applicability of autoconfiguration requirements to Host/Workstation

Paragraph	Type of Edit	Change from v2.0 to v3.0
3.1.3.1	Update	Privacy addressing for Advanced Server made conditional, only applies when the Server is acting as a client AND requires anonymity
3.2.1	Clarification	Specific citation of limited router requirements for SLAAC (RFC 4862)
3.2.1	Addition	Conditional requirements for Router deployed as DHCPv6 Server or Relay Agent
3.2.1	Update	Reduce tunneling requirements to Conditional MUST
3.2.2	Addition	Conditional requirement for L3 Switch deployed with interior router capability
3.2.3	Addition	Introductory paragraphs
3.2.3.3	Addition	Added section on HAIPE
App C	Updates	Added a column for “effective date” for new/revised RFCs; made table changes consistent with updates in the text
App C	Correction	Missing row for RFC 3633 which is tied to RFC 3769 as stated in paragraph 2.9.3
App C	Correction	Replace table reference to RFC 4309 with a reference to IEEE 802.11-2007i consistent with an earlier change in the text
App D	Editorial	Merge change logs of interim versions v2.1 and v2.2 to reflect all changes from v2.0 baseline to v3.0; resort and eliminate redundant or reversed entries
Various	Editorial	Clarification of language, punctuation, etc. as pointed out by reviewers and discovered in final check

Appendix E: IPsec and IKE RFC References

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Header	Function	Algorithm	RFC	RFC 4835	RFC 4308 VPN-B	RFC 4869 Suite-B-GCM-128	RFC 4869 Suite-B-GMAC-128	RFC 4307	DoD IPv6 v1.0	DoD IPv6 v2.0	DoD IPv6 v3.0	NIST IPv6 v1 draft 2
2	ESP	encryption	NULL	2410	MUST				MAY	MUST	MUST	MUST	MUST
3	ESP	encryption	AES-CBC-128	3602	MUST	MUST				MUST	MUST	MUST	MUST
4	ESP	integrity	HMAC-SHA1-96	2404	MUST					MUST	MUST	MUST	MUST
5	AH	integrity	HMAC-SHA1-96	2404	MUST					MUST	MUST	MUST	MUST
6	IKEv2	integrity	HMAC-SHA1-96	2404					MUST	SHOULD+	MUST	MUST	MUST
7	ESP	integrity	AES-XCBC-MAC-96	3566	SHOULD+					SHOULD+	SHOULD+	SHOULD+	SHOULD+
8	AH	integrity	AES-XCBC-MAC-96	3566	SHOULD+					SHOULD+	SHOULD+	SHOULD+	SHOULD+
9	IKEv2	encryption	AES-CBC-128	3602		MUST	MUST	MUST	SHOULD+	SHOULD+	SHOULD+	MUST	MUST
10	IKEv2	pseudo random	AES-XCBC-PRF-128	4434		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
11	IKEv2	integrity	AES-XCBC-MAC-96	3566		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
12	IKEv2	diffie-hellman	2048-bit MODP	3526		MUST			SHOULD+	SHOULD+	SHOULD+	SHOULD+	SHOULD+
13	ESP	encryption/integrity	AES-CBC-128 16-octet ICV GCM	4106			MUST	MUST			SHOULD+	MUST	
14	ESP	integrity	NULL	4303	MAY		MUST	MUST		MUST	SHOULD+	MUST	Discouraged
15	IKEv2	pseudo random	HMAC-SHA-256	4868			MUST	MUST			SHOULD+	MUST	SHOULD+
16	IKEv2	integrity	HMAC-SHA-256-128	4868			MUST	MUST			SHOULD+	MUST	SHOULD+
17	IKEv2	diffie-hellman	256-bit random ECP	4753			MUST	MUST			SHOULD+	MUST	
18	IKEv2	authentication	ECDSA-256	4754			MUST	MUST			SHOULD+	MUST	
19	IKEv2	pseudo random	PRF-HMAC-SHA1	2401					MUST	SHOULD+	MUST	MUST	MUST
20	ESP	encryption	3DES-CBC	2451	MUST				MUST	MUST	MUST	MUST	MUST
21	IKEv2	encryption	3DES-CBC	2451					MUST				MUST
22	SEND			3971						SHOULD+	SHOULD	SHOULD	
23	CGA			3972						SHOULD+	SHOULD	SHOULD	
24	SLAAC		privacy extensions	3041						SHOULD	SHOULD	OBS	
25	SLAAC		privacy extensions	4941								SHOULD	
26	IPsec	key mgmt	manual key management	4301						MUST	MUST	MUST	
27	IKEv2	key mgmt	IPsec Certificate Management Profile	4809									SHOULD+
28	IKEv2	key mgmt	IPsec PKI Profile	4945									SHOULD+
29	ESP	encryption	AES-CTR-128	3686	SHOULD				SHOULD				SHOULD
30	ESP	integrity	HMAC-SHA-256-128	4868									SHOULD+
31	AH	integrity	HMAC-SHA-256-128	4868									SHOULD+